ESCUELA DE POSGRADO
UNIVERSIDAD CÉSAR VALLEJO

Gestión de riesgos de TI en la seguridad de la información del Programa de Desarrollo Productivo Agrario Rural 2017

TESIS PARA OPTAR EL GRADO ACADÉMICO DE:

MAESTRO EN GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN

AUTOR:

Br. Otoya Verástegui Melitón Ricardo

ASESOR:

Dr. Willian Sebastián Flores Sotelo

SECCIÓN:

Ingeniería

LÍNEA DE INVESTIGACIÓN:

Proyectos de Tecnologías de la Información

PERÚ – 2018

Página del Jurado

Presidente

Dr. César Humberto Del Castillo Talledo

Secretario

Dr. Willian Sebastian Flores Sotelo

Vocal

Dedicatoria

A mis queridos padres Mélito y Maruja; Nelda mi madrina que en vida me brindo todo su apoyo y fortaleza.

Agradecimiento

A todos los docentes de la Escuela de Postgrado de la “Universidad César Vallejo” por su valiosa enseñanza y permanente orientación, durante nuestros estudios de Maestría, al Dr. Willian Sebastian Flores Sotelo, por su asesoría; y a los colaboradores del Programa de Desarrollo Productivo Agrario Rural; por su valiosa colaboración durante el desarrollo de la presente investigación.

Declaratoria de autenticidad

Yo, Melitón Ricardo Otoya Verástegui, estudiante del Programa de Maestría en Gestión de Tecnologías de la Información de la Escuela de Postgrado de la Universidad César Vallejo, identificado con DNI N°19336295, respectivamente, con la tesis titulada "Gestión de riesgos de TI en la seguridad de la información del Programa de Desarrollo Productivo Agrario Rural 2017", declaro bajo juramento que:

1) La tesis es de autoría propia.

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

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

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

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

Los Olivos, 18 de febrero del 2018

_____

Melitón Ricardo Otoya Verástegui

DNI: 19336295

Presentación

Señores miembros del jurado calificador

De conformidad con el Reglamento de Grados y Títulos de la Universidad César Vallejo, pongo a vuestra consideración la evaluación de la tesis "Gestión de Riesgos de TI en la seguridad de la Información del Programa de Desarrollo Productivo Agrario Rural 2017" elaborada con el objetivo general de conocer en qué medida una gestión de riesgos de TI influye en la seguridad de la información del Programa de Desarrollo Productivo Agrario Rural 2017.

En el presente trabajo, se estudia la identificación, análisis y tratamiento del riesgo de TI en la seguridad de la información de Programa de Desarrollo Productivo Agrario Rural. El estudio comprende los siguientes capítulos: el capítulo I se refiere a la introducción, que contiene antecedentes, fundamentación científica, técnica o humanística, justificación, problema, hipótesis, objetivos; el capítulo II se refiere al Marco metodológico, el cual comprende la operacionalización de las variables, la metodología, tipos de estudio, diseño de investigación, la población y muestra, las técnicas e instrumentos de recolección de datos y los métodos de análisis de datos. ; el capítulo III aborda los resultados; el capítulo IV se refiere a la discusión; el capítulo V a las conclusiones; el capítulo VI a las recomendaciones. Por último, el capítulo VII menciona las referencias bibliográficas y los anexos respectivos.

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

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

Los Olivos, 18 de febrero del 2018

_____

Melitón Ricardo Otoya Verástegui

DNI: 19336295

Índice de contenido

Página del Jurado ii
Declaratoria de autenticidad v
Presentación vi
Índice de contenido vii
Resumen xi
Abstract xii
I. Introducción 13
1.1 Realidad problemática 14
1.2 Trabajos previos 18
1.2.1 Trabajos previos internacionales 18
1.2.2 Trabajos previos nacionales 21
1.3 Fundamentación científica, técnica o humanística 25
1.3.1 Conceptualización variable independiente: Gestión de Riesgos 25
1.3.2 Base teórica de la variable independiente: 28
1.3.3 Conceptualización variable dependiente: Seguridad de la información 47
1.3.4 Base teórica de la variable dependiente: Seguridad de la Información 49
1.4 Formulación del problema 66
1.4.1 Problema general 67
1.4.2 Problemas específicos 68
1.5 Justificación del estudio 68
1.5.1 Justificación teórica 68
1.5.2 Justificación practica 69
1.5.3 Justificación metodológica 69
1.5.4 Hipótesis general 70
1.5.5 Hipótesis especificas 70
1.6 Objetivos 71
1.6.1 Objetivo general 71
1.6.2 Objetivos específicos 71
II. Marco metodológico 73
2.1 Variables 74
2.2 Operacionalización de variables 76
2.3 Metodología 77
2.4 Tipo de estudio 77
2.5 Diseño 77
2.6 Población, muestra y muestreo 78
2.7 Técnicas e instrumentos de recolección de datos 80

2.8 Métodos de análisis de datos 83
III. Resultados 85
3.1 Resultados descriptivos. 86
IV. Discusión 99
V. Conclusiones 104
VI. Recomendaciones 108
VII. Referencias 111
VIII. Anexos 117

Índice de tablas

Tabla 1	Matriz de operacionalización de la variable gestión de riesgos	76
Tabla 2	Matriz de operacionalización de la variable seguridad de la información	76
Tabla 3	Número de colaboradores que conforman la muestra de estudio, según oficinas y direcciones	80
Tabla 4	Juicio de expertos	82
Tabla 5	Confiabilidad de los instrumentos - Alfa de Cronbach	83
Tabla 6	Niveles de la gestión de riesgos de TI del Programa de Desarrollo Productivo Agrario Rural 2017	86
Tabla 7	Niveles de la seguridad de la información en Agrorural 2017.	87
Tabla 8	Ajuste de los datos para el modelo de la gestión de riesgos de TI en la seguridad de la información del Programa de Desarrollo Productivo Agrario Rural 2017.	88
Tabla 9	Determinación de las variables para el modelo de regresión logística ordinal.	89
Tabla 10	Estimación de parámetros de la gestión de riesgos en la seguridad de la información del Programa de Desarrollo Productivo Agrario Rural 2017.	89
Tabla 11	Prueba de hipótesis general.	90
Tabla 12	Estimación de parámetros de la gestión de riesgos de los activos de información en la seguridad de la información del Programa de Desarrollo Productivo Agrario Rural 2017.	91
Tabla 13	Prueba de hipótesis especifica 1.	92
Tabla 14	Estimación de parámetros de gestión de riesgos de las amenazas de TI en la seguridad de la información del Programa de Desarrollo Productivo Agrario Rural 2017.	93
Tabla 15	Prueba de hipótesis especifica 2.	94
Tabla 16	Estimación de parámetro del impacto potencial de ejecución riesgos en la seguridad de la información en el Programa de Desarrollo Productivo Agrario Rural 2017	94
Tabla 17	Prueba de hipótesis especifica 3.	95
Tabla 18	Estimación de parámetro de riesgos potenciales en la seguridad de la información del Programa de Desarrollo Productivo Agrario Rural 2017.	96
Tabla 19	Prueba de hipótesis especifica 4	97
Tabla 20	Estimación de parámetros de los salvaguardas para los riesgos de TI en la seguridad de la información del Programa de Desarrollo Productivo Agrario Rural 2017.	97
Tabla 21	Prueba de hipótesis especifica 5.	98

Índice de figuras

Figura 1.	Gestión de riesgos	30
Figura 2.	Proceso de gestión de riesgos	31
Figura 3.	Elementos del análisis de riesgos potenciales	33
Figura 4.	Decisiones de tratamiento de los riesgos	35
Figura 5.	Zonas de riesgo	37
Figura 6.	Seguridad de la información	53
Figura 7.	Planos de actuación en la seguridad de la información	55
Figura 8.	Seguridad informática como proceso y no como producto	56
Figura 9.	Modelo para la gestión de la seguridad de la información	59
Figura 10.	Niveles de madurez de la SGSI en la organización	61
Figura 11.	Niveles de la gestión de riesgos en AGRORURAL	86
Figura 12	Niveles de la seguridad de la información en Agrorural	87
Figura 13.	Representación del área COR, como incidencia de la gestión de riesgos en la seguridad de la información.	91

Resumen

El siguiente trabajo, tiene como propósito garantizar que los riesgos de TI puedan ser identificados y controlados, es decir se debe realizar una adecuada "Gestión de riesgos" en la seguridad de la información del Programa de Desarrollo Productivo Agrario Rural 2017.

La gestión de riesgos de TI permitirá a los profesionales en tecnologías de la información una mejor gestión tecnológica, dado que contara con las herramientas para la mejor toma de decisiones en escenario de riesgos y amenazas. Implica la consideración de las causas y las fuentes de riesgo en TI, sus consecuencias positivas y negativas y la probabilidad de que estas consecuencias puedan ocurrir. Dicha gestión de riesgos de TI permitirá establecer valores y dimensiones de los activos; así como las consecuencias del impacto de una amenaza o probabilidad de la ejecución de un riesgo para una adecuada implantación de seguridad de la información asegurando la continuidad operativa de la institución.

Por lo que la investigación mide la influencia de la gestión de riesgos de TI en la seguridad de la información el Programa de Desarrollo Agrario Rural 2017.

Palabras clave (3): *Gestión de riesgos, seguridad de la información, continuidad operativa*

Abstract

The following work has the purpose of guaranteeing that the IT risks can be identified and controlled, that is, an adequate "Risk Management" must be carried out in the information security of the Rural Agricultural Productive Development Program 2017.

IT risk management will allow professionals in information technology a better technological management given that they will have the tools for the best decision making in the scenario of risks and threats. It involves the consideration of the causes and sources of risk in IT, its positive and negative consequences and the probability that these consequences may occur. Such IT risk management will allow to establish values and dimensions of the assets; as well as the consequences of the impact of a threat or probability of the execution of a risk for an adequate implementation of information security, ensuring the operational continuity of the institution.

Therefore, the research measures the influence of IT risk management on information security in the 2017 Rural Agrarian Development Program.

Keywords (3): *Risk management, information security, operational continuity*

I. Introducción

1.1 Realidad problemática

Moreno y Camacho (2011) consideraron que “el riesgo tecnológico no es clasista, existe en todas partes del mundo y afecta tanto a los países ricos como a países pobres y en vías de desarrollo” (p. 43), por lo general, poca o ninguna advertencia antecede a los incidentes relacionados con riesgos tecnológicos, en muchos casos, las víctimas no saben si han sido afectadas sino hasta muchos años después, los procesos que involucran tecnologías implican un constante evolucionar marcado por cambios en periodos muy cortos de tiempo, lo que permite considerar que los entornos tecnológicos no son estables, ejemplos evidentes los tenemos en las tecnologías de la información y comunicaciones y la biotecnología, cuyo tiempo de modificación y cambio es bastante elevado. Ha mediado de los años 80, el sector empresarial reconoció la importancia de los riesgos tecnológicos, lo que obligó a la integración de estos con los procesos de planificación y calidad a partir de metodologías compuestas de gestión de riesgos, considerando su incidencia sobre los costos derivados de la actividad empresarial. Como resultado del acelerado ritmo asociado a las actividades tecno-científicas, surgen amenazas de orden tecnológico y por consiguiente se reconoce la existencia de riesgos de carácter técnico y la necesidad de integrarlos a la cosmovisión producto de estas actividades; por lo que hay que enfilar esfuerzos en generar una conciencia basada en el conocimiento de los riesgos tecnológicos en los sistemas de información.

La variable independiente de gestión de riesgos está en una base incipiente como base para una buena seguridad de la información en el Programa de Desarrollo Productivo Agrario Rural, por lo que una buena implementación de gestión del riesgo consiste en un proceso cíclico que se inicia a partir de un conjunto de información recogida de diversas fuentes (requisitos, personas, procesos de desarrollo, presupuestos, expectativas, etcétera). Toda esta información proporciona una lista de riesgos a tener en cuenta que permitirá organizar concienzuda y prudente la defensa para que no pase nada malo y al mismo tiempo estar preparados para atajar las emergencias, sobrevivir a los incidentes y seguir operando en las mejores condiciones.

> De acuerdo a Magerit (2012), nos explicó que nada es perfecto, se dice que el riesgo se reduce a un nivel residual que la dirección puede asumir, es por ello que para poder medir dicho impacto en la institución de estudio se ha identificado las siguientes dimensiones: (1) Activos de información, que son los elementos del sistema de información (o estrechamente relacionados con este) que soportan la misión de la institución, (2) Amenazas, que son las cosas que les pueden pasar a los activos causando un perjuicio a la institución, (3) Impacto potencial, lo que podría pasar, es la medida del daño sobre el activo derivado de la materialización de una amenaza, conociendo el valor de los activos (en varias dimensiones) y la degradación que causan las amenazas, es directo derivar el impacto que estas tendrían sobre el sistema (4) Riesgo potencial, lo que probablemente pase; es la medida del daño probable sobre un sistema, conociendo el impacto de las amenazas sobre los activos, es directo derivar el riesgo sin más que tener en cuenta la probabilidad de ocurrencia, (5) Salvaguardas, (o corta medidas) que son medidas de protección desplegadas para aquellas amenazas no causen tanto daño. (p. 22).

Al observar el entorno del Programa de Desarrollo Productivo Agrario Rural, se puede percibir la influencia que ejercen las distintas tecnologías sobre éste y lo vulnerable que se encuentra ante la amenaza caracterizada durante los últimos años, por diversos eventos adversos de origen tanto natural, como antrópico y que han servido para revelar la poca capacidad existente en las diversas áreas de la institución para gestionar y responder de manera integral, ante escenarios de riesgos tecnológicos. Existe poco o casi nulo análisis de los procesos críticos tecnológicos que deben tener sus riesgos identificados, evaluados, monitoreados y controlados; así como también se evidencia que no se hace uso de ninguna metodología de gestión de riesgos que garantice la continuidad operativa de la institución que tiene como fin velar por la correcta y oportuna atención a los proyectos de desarrollo agrario rural a nivel nacional.

Propósito de la investigación

El propósito de la presente investigación en el Programa de Desarrollo Productivo Agrario Rural tiene una importancia relevante dado que al usar tecnología en su actividad diaria y como parte de sus procesos de negocio se encuentran expuestas a todo tipo de riesgos; por ello pueden afectar la actividad propia de las mismas y ser fuentes de pérdidas y daños considerables. De lo anterior los planes de seguridad deben enfatizar en crear conciencia en seguridad para prevenir riesgos y buscar estrategias para obtener el apoyo de la alta dirección con el fin de cumplir con los objetivos y asegurar la información crítica, adicional a la gestión adecuada de los riesgos debe permitir evitar en gran medida la ocurrencia de incidentes y con ello evitar la activación de planes de continuidad. La de gestión de riesgos en los sistemas de información, permitirá conocer los riesgos y amenazas a las que se encuentra expuesta los activos informáticos en la institución, y sobre todo se podrá saber el impacto que causaría a cada uno de ellos, en el caso de que las amenazas se llegaran a Materializar.

Problemática de la institución evaluada

Agrorural vela por la correcta atención de servicios públicos agrarios, en este contexto es de vital importancia el manejo de la información de forma adecuada y oportuna para las mejores decisiones, por lo es necesario identificar, analizar y tratar los riesgos tecnológicos que permitan un adecuado sistema de seguridad de la información que asegure la continuidad operativa y poder contar con la disponibilidad de la información de manera confidencial e integra. Existe la disponibilidad y obligatoriedad de establecer el SGSI (sistema de gestión de seguridad de la información) según la (ONGEI, 2009) pero hay poca importancia de desarrollar planes de actividades de planificación requeridas por la norma de manera metodológica y en concordancia con la política y objetivos del SGSI dentro del alcance del mismo en las diferentes Instituciones Nacionales de la cual no es ajena Agrorural, por lo que la seguridad de la información necesita de un proceso de gestión del riesgo es decir, una aplicación sistemática de políticas, procedimientos y prácticas de gestión a las actividades de comunicación, consulta, establecimiento del contexto, e identificación, análisis, evaluación, tratamiento, seguimiento y revisión del riesgo.

La seguridad de la información en Agro rural es un pilar importante ya que está estrechamente relacionado a los objetivos estratégicos por ello tiene vital importancia una buena implementación de un sistema de gestión de la seguridad de la información; (Santos, 2014) nos dijo que: “al ser la seguridad un concepto asociado a la certeza, falta de riesgo o contingencia. Conviene aclarar que no siendo posible la certeza absoluta, el elemento de riesgo está siempre presente” (p. 11), independientemente de las medidas que tomemos, por lo que debemos hablar de niveles de seguridad, la seguridad absoluta no es posible y en adelante entenderemos que la seguridad informática es un conjunto de técnicas encaminadas a obtener altos niveles de seguridad en los sistemas informáticos, podemos entender como seguridad una característica de cualquier sistema que nos indica que ese sistema está libre de todo peligro, daño o riesgo, y que es, en cierta manera, infalible. Como esta característica, particularizando para el caso de sistemas informáticos, sistemas operativos o redes de computadores, es muy difícil de conseguir (según la mayoría de expertos, imposible), se suaviza la definición de seguridad y se pasa a hablar de fiabilidad, probabilidad de que un sistema se comporte tal y como se espera de él. Por tanto, se habla de tener sistemas fiables en lugar de sistemas seguros.

Se ha tomado en cuenta la medición de esta variable a través de las siguientes dimensiones:

> Según Gómez (2014), definió cuatro dimensiones: (1) Técnico, tanto a nivel físico y lógico como selección, instalación, configuración y actualización de soluciones de hardware y software, criptografía, estandarización de productos, desarrollo seguro de aplicaciones, (2) Legal, cumplimiento y adaptación a la legislación vigente, ley de protección de datos, ley de delitos informáticos, firma electrónica, código penal, propiedad intelectual, directivas establecidas por la secretaria de gobierno digital de la PCM, etcétera, (3) Humano, sensibilización y formación, funciones, obligaciones y responsabilidades del personal, control y supervisión de los empleados, (4) Organizativo, Políticas, normas y procedimientos,

> planes de contingencia y respuesta a incidentes, relaciones con terceros (clientes y proveedores). (p. 46).

Presentación del proyecto de investigación

Actualmente el Programa de Desarrollo Productivo Agrario rural cuenta con 174 colaboradores laborando en la sede central los cuales necesitan intercambiar información para realizar sus labores cotidianas como por ejemplo el uso ininterrumpido del internet, el correo electrónico institucional, su seguridad perimetral contra cualquier ataque informático, la conectividad en línea con sus sedes, la accesibilidad de los sistemas en web y que seguridad se proporciona a los mismos. Entonces la continuidad del negocio tecnológico se basa en la adecuada implementación de un sistema de gestión de seguridad de información que necesita de una aplicación de políticas y lineamientos del mismo basado en una identificación, análisis y tratamiento de los riesgos tecnológicos, para lo cual nos respaldaremos en la aplicación de las ISO 27001:2013 sistema de seguridad de la información (Indecopi, 2014), la ISO 31000 gestión de riesgos (Inacal, 2011), la metodología de Magerit orientados a la consecución de los objetivos estratégicos de la institución.

Bonilla y González (2012) dijo: “en vista de la necesidad de tener un diseño de seguridad adecuado para la organización y un retorno de la inversión a corto plazo, se debe implementar un diseño de seguridad eficiente” (p. 14), para esto es fundamental hacer correctamente la identificación y análisis de los riesgos de la organización. Al tener claro los riesgos más significativos y qué se debe proteger, se puede implementar un diseño de seguridad sin necesidad de hacer inversiones en equipos que no se requieren, esto sin descuidar la protección para el buen funcionamiento de la organización. No basta implementar un buen sistema de seguridad donde se incluyen los controles, arquitectura y políticas, si no se realiza un seguimiento, monitoreo y evaluación de la solución implementada, ya que solo las herramientas no hacen el trabajo, por ello es importante la verificación continua y los ajustes que se le puedan realizar.

1.2 Trabajos previos

1.2.1 Trabajos previos internacionales

Molina (2015) *Propuesta de un plan de gestión de riesgos de tecnología aplicado en la Escuela Superior Politécnica del Litoral.* Tesis para obtener el grado de master en ingeniería de redes y servicios telemáticos en la Universidad Politécnica de Madrid España, cuyo problema fue la necesidad de desarrollar un plan de gestión de riesgo para mitigar las fallas y amenazas que atentan contra la seguridad de los equipos y de la información en la Escuela superior Politécnica del Litoral. El objetivo fue el de Desarrollar un plan de gestión de riesgos tecnológicos aplicado al centro que administra y brinda los servicios de red y sistemas a la Escuela superior Politécnica del Litoral, se usó Magerit, como metodología para conocer las amenazas a los cuales se encuentran expuestos los activos que forman parte del departamento de informática de la ESPOL, el tipo de estudio que se uso es descriptivo, el diseño no experimental y el enfoque cualitativo, utilizó la técnica de la entrevista y observación. El instrumento usado fue la guía de entrevista y lista de cotejo, los resultados obtenidos tras la evaluación del nivel de degradación y frecuencia en que podrían materializarse las amenazas sobre los activos, demuestran que los niveles de riesgos presentes son medio y alto, el autor concluyo que la herramienta PILAR permitió ingresar las valoraciones para realizar las evaluaciones referentes a los activos, amenazas y salvaguardas para finalmente obtener los niveles de riesgo e impacto plasmados en gráficas radiales permitiendo identificar fácilmente la necesidad de implementar procedimientos y normas cuya finalidad sea la protección de los recursos e información.

Guillén (2014) *Planteamiento del modelo de gestión del riesgo para empresas de reprocesamiento de dispositivos de ortodoncia, apoyado en TI.* Tesis para obtener el obtener el título de magister en gerencia de sistemas y tecnologías de la información en la Universidad de las Américas, Quito Ecuador. El problema fue como evaluar las exigencias normativas de riesgos creando un modelo de gestión de riesgos con una arquitectura modular, basado en los principios de normativas y estándares internacionales, estudios especializados y mejores prácticas de manejo de riesgos. El objetivo fue el diseñar un modelo del riesgo que pueda ser utilizado en los procesos de reprocesamiento para empresas de reprocesamiento de dispositivos de ortodoncia, el tipo de estudio que se uso es descriptivo, el diseño no experimental y el enfoque cualitativo, utilizó la técnica de la encuesta, entrevista y observación. El instrumento usado fue el cuestionario, la

guía de entrevista y lista de cotejo, los resultados obtenidos permitieron a los actores del riesgo identificar, analizar, evaluar, monitorizar, dar tratamiento y realizar revisiones de sus riesgos de forma integrada, en una misma herramienta de fácil e intuitivo uso, El autor concluyo que el manejo de riesgos y calidad son indispensables en compañías dedicadas al reprocesamiento de dispositivos de ortodoncia, ya que su actividad de fabricación produce dispositivos que serán utilizados para la salud humana y se debe promover la salud, requiriéndose contar con procesos controlados y estandarizados.

Burgos (2014) *Elaboración del plan de gestión de riesgos de las tecnologías de la información para Roche Ecuador S. A. en la ciudad de Quito, provincia de Pichincha, para el año 2014.* Tesis para obtener el obtener el título de magister en gerencia de sistemas y tecnologías de la información en la Universidad de las Américas, Quito Ecuador, el problema fue implementar un modelo de gestión de riesgos de TI acorde a la organización para minimizar las vulnerabilidades de los activos del área de tecnología de la información, en la empresa Roche. El objetivo fue diseñar un plan de gestión de riesgos para Roche Ecuador S.R. apalancado por los estándares aplicables a dicho efecto, con la finalidad de influir positivamente en la eficacia y eficiencia operativa de la compañía, el tipo de estudio que se uso es descriptivo, el diseño no experimental y el enfoque cualitativo - cuantitativo, la población usada fue de 150 colaboradores de la empresa Roche, se utilizó la técnica de la encuesta, entrevista y observación. El instrumento usado fue el cuestionario, la guía de entrevista y lista de cotejo, los resultados obtenidos permitieron conocer las vulnerabilidades que podían convertirse en amenazas, estableciendo una metodología de gestión de riesgo como alternativa optima de solución y control, el autor concluyo que la alternativa optima de solución para los problemas señalados fue la implementación de un modelo general de gestión de riesgos de TI.

Fernández (2014) *Propuesta metodológica para la gestión de riesgos tecnológicos de empresas proveedoras de servicios de telecomunicaciones.* Tesis para obtener el obtener el grado de maestría en evaluación y auditoria de sistemas tecnológicos en la Universidad de las Fuerzas Armadas, Quito Ecuador. El problema fue medir el nivel de la gestión de riesgos en las empresas

proveedoras de servicios de Internet en la ciudad de Quito. Su objetivo fue elaborar una propuesta metodológica de gestión del riesgo tecnológico para empresas del sector de las telecomunicaciones dedicadas a la provisión del servicio de internet (ISP), el tipo de estudio que se uso es descriptivo, el diseño no experimental y el enfoque cualitativo, se utilizó la técnica de la encuesta, entrevista y observación. El instrumento usado fue el cuestionario, la guía de entrevista y lista de cotejo, los resultados obtenidos del modelo aplicado fue de disponer de información para tomar decisiones conociendo los activos a proteger, las amenazas y salvaguardas valoradas, los cuales no eran los óptimos para una adecuada gestión del riesgo, el autor concluyo que el grado de madurez de los ISP de la ciudad de Quito, como administran sus riesgos tecnológicos está por debajo de un valor que pueda considerarse "administrable".

Maggiori (2014) *Modelo de Evaluación de Madurez para la Gestión de la Seguridad de la Información Integrada en los Procesos de Negocio.* Tesis para obtener el obtener el grado de maestría en seguridad informática en la Universidad de Buenos Aires, Buenos Aires Argentina. El problema fue seleccionar un modelo de madurez para la evaluación de la gestión de riesgos, de la gestión de seguridad de la información y del plan/programa de seguridad de la información, integrados en el negocio. El objetivo diseñar e implementar un modelo para la evaluación de madurez de la gestión de la seguridad de la información integrada en los procesos de negocio, así como los riesgos asociados al uso de la información y los controles definidos para su tratamiento, el tipo de estudio que se uso es descriptivo, el diseño no experimental y el enfoque cualitativo, se utilizó la técnica de la encuesta, entrevista y observación. El instrumento usado fue el cuestionario, la guía de entrevista y lista de cotejo, los resultados obtenidos fue la implementación del modelo CMMI, como el camino a seguir para lograr la madurez de la gestión de la seguridad de la información, el autor concluyo que es necesario la integración de la evaluación de riesgos de seguridad de la información en la evaluación de riesgos de negocio, así como de redefinir el plan de seguridad de la información.

1.2.2 Trabajos previos nacionales

Huamán (2017) *Plan de Comunicaciones en Seguridad de la Información para el*

personal administrativo de la Pontificia Universidad Católica del Perú. Tesis para obtener el grado de magister en comunicaciones, Pontificia Universidad Católica del Perú Lima Perú. El problema se enmarcaba en toda la comunidad universitaria de la PUCP (es decir: docentes, administrativos y alumnos), respecto al nivel de cultura de seguridad de la información, su objetivo fue construir para el 2016 las bases para la cultura de seguridad de la información en el personal administrativo de la PUCP a través de la concientización del problema, las buenas prácticas en el uso y manejo de la tecnología (entrenamiento) y mediante sus comportamientos (educación) para garantizar la protección y resguardo de la información de la Universidad, el tipo de estudio que se uso es descriptivo, el diseño no experimental y el enfoque cualitativo, se utilizó la técnica de la encuesta, entrevista y observación. El instrumento usado fue el cuestionario, la guía de entrevista y lista de cotejo, como resultado se obtuvo la medición de actividades y/o productos a través de indicadores del nivel de cultura de seguridad de la información en el personal administrativo de la PUCP, el autor concluyo que el personal administrativo conoce y maneja, en un 50% más, los conceptos básicos en seguridad de la información logrando el objetivo al 100% respecto al objetivo específico, lo que permite el inicio de la estructura base de conocimientos clave para construir la cultura de seguridad de la información en la PUCP.

Mercado (2016) *Modelo de Gestión de seguridad de la información para el E – Gobierno.* Tesis para optar el Grado Académico de Magíster en Ingeniería de Sistemas con mención en Gestión de la Tecnología de Información y Comunicaciones en la Universidad Nacional Mayor de San Marcos, Lima Perú. El problema fue que no se contaba con un modelo de gestión de seguridad de la información que orienten la implementación y supervisión de la seguridad de la información en los servicios de gobiernos electrónicos brindados por las entidades del sector público. El objetivo fue Elaborar un modelo de gestión de seguridad de la información para el gobierno electrónico en las entidades públicas, el tipo de estudio que se uso es descriptivo, el diseño no experimental y el enfoque cualitativo, se utilizó la técnica de la encuesta, entrevista y observación. El instrumento usado fue el cuestionario, la guía de entrevista y lista de cotejo, como resultado se obtuvo que luego de la aplicación de la metodología de gestión de riesgo, se ha elaborado el documento de declaración de aplicabilidad, en el cual

se ha justificado los controles que se va a implementar y los que no de acuerdo a lo establecido por el modelo GSI-E-Gob, el autor concluyó que el modelo permite medir la seguridad global de los procesos que brindan servicio de gobierno electrónico en relación a los controles de seguridad con los que se cuenta, lo cual genera una tendencia hacia la mejora continua.

Saavedra (2015) *Diseño e implementación de un sistema integrado de gestión de equipos de seguridad.* Tesis para optar el Título de Magister en Ingeniería de las Telecomunicaciones en la Pontificia Universidad Católica del Perú Lima Perú. El problema fue que no existía una buena gestión de redes para reducir al mínimo la frecuencia y el impacto en el negocio de las condiciones que reducen la disponibilidad o el rendimiento de la infraestructura de red. El objetivo fue la implementación de una herramienta integral de gestión de equipos de seguridad informática para reducir al mínimo la frecuencia y el impacto en el negocio de las condiciones que reducen la disponibilidad, o el rendimiento de la infraestructura de red, el tipo de estudio que se uso es descriptivo, el diseño no experimental y el enfoque cualitativo, se utilizó la técnica de la encuesta y observación. El instrumento usado fue el cuestionario y lista de cotejo, el resultado obtenido fue una herramienta gráfica de monitoreo de red basada en lenguaje de programación PHP para recoger datos de los dispositivos de red, almacenando dicha información en una base de datos Mysql que es presentada al usuario mediante una interfaz web haciendo uso de un servidor APACHE, el autor concluye que con la implementación del sistema de gestión, se logró obtener una herramienta de monitoreo, que en base a su diseño funcional nos permite anticipar posibles fallas de funcionamiento y mejorar los tiempos de respuesta frente a incidencias.

Neuhaus (2013) *Identificación de factores que limitan una implementación efectiva de la gestión del riesgo de desastres a nivel local, en distritos seleccionados de la región de Piura.* Tesis para optar el grado de Magíster en Gerencia Social en la Pontificia Universidad Católica del Perú Lima Perú. El problema fue que el enfoque de la gestión del riesgo de desastres, implementado por ley en los diferentes niveles administrativos del Estado, era tan poco efectivo, el objetivo fue Identificar algunos factores que estarían limitando una

implementación efectiva de la gestión del riesgo de desastres en gobiernos distritales seleccionados en la región de Piura, para proponer medidas orientadas a fortalecer la gestión de riesgo de desastres a nivel local y brindar insumos en el marco de la nueva ley que crea el Sistema Nacional de Gestión de Riesgo y Desastres, el tipo de estudio que se uso es descriptivo, el diseño no experimental y el enfoque cualitativo, se utilizó la técnica de la encuesta, entrevista y observación. El instrumento usado fue el cuestionario, la guía de entrevista y lista de cotejo, el resultado que se obtuvo de este estudio fue que existe una pobre implementación de la gestión del riesgo de desastres en los distritos seleccionados de la región Piura, el autor concluye que en el país existe poca cultura de prevención. La actual estrategia de incentivar y difundir una cultura de prevención y de gestión del riesgo de desastres en el país no es efectiva en cuanto a generar compromiso con la temática.

Calderón (2012) *Análisis e Implementación de un Sistema de Gestión de Riesgos para la prevención de accidentes en la mina EL BROCAL S.A.A Unidad Colquijirca Pasco.* Tesis para optar el grado de maestro en ciencias con mención en seguridad y salud minera en la Universidad Nacional de Ingeniería Lima Perú. El problema fue que el trabajo que realizaban los trabajadores de la mina Colquijirca era empírico, su conocimiento técnico era regular, los conceptos y principios de seguridad eran incipientes; y las últimas estadísticas de seguridad reportan altos índices de accidentabilidad, el objetivo fue Diseñar, identificar y aplicar un Sistema de Gestión de Riesgos con la finalidad de tener personal preparado para el trabajo minero y mejorar su calidad de vida, el tipo de estudio que se uso es descriptivo, el diseño no experimental y el enfoque cualitativo, se utilizó la técnica de la encuesta y observación. El instrumento usado fue el cuestionario y lista de cotejo, el resultado obtenido fue el diseño del modelo del Sistema de Seguridad y Salud Ocupacional, el autor concluye que el ISO 31000 es una herramienta que permite la mejora en la gestión de riesgos en la seguridad en el trabajo de las organizaciones y se recomienda que las empresas trabajan e incorporen del ISO 9000, ISO 14001, OSHAS 18001 y se integren al ISO 31000. Para una mejora continua de su organización.

1.3 Fundamentación científica, técnica o humanística

1.3.1 Conceptualización variable independiente: Gestión de Riesgos

Piattini y Del Peso (2001) definió que en la “gestion de riesgos se trata de identificar los riesgos, cuantificar su probabilidad e impacto, y analizar medidas que los eliminen, lo que generalmente no es posible, o que disminuyan la probabilidad de que ocurran los echos o mitiguen el impacto” (p. 132), para evaluar riesgos hay que considerar, entre otros factores, el tipo de información almacenada, procesada y transmitida, la criticidad de las aplicaciones, la tecnología usada, el marco legal aplicable, el sector de la entidad, la entidad misma y el momento. Desde la perspectiva de la auditoria de la seguridad es necesario revisar si se han considerado las amenazas, o bien evaluarlas si es el objetivo, y de todo tipo: errores y negligencias en general, desastres naturales, fallos de instalaciones, o bien fraudes o delitos, y que pueden traducirse en daños a: personas, datos, programas, redes, instalaciones, u otros activos, y llegar a suponer un peor servicio a usuarios internos y externos, estos normalmnete clientes, imagen degradada u otros dificilmente cuantificables, e incluso perdida irreversible de datos, y hasta el fin de la actividad de la entidad en los casos mas graves.

> Gomez (2014) nos dijo: un proceso de gestión de riesgos comprende una etapa de evaluación previa de los riesgos del sistema informático, que se debe realizar con rigor y objetividad para que cumpla su función con garantías. Para ello, el equipo responsable de la evaluación debe contar con un nivel adecuado de formación y experiencia previa, así; como disponer de una serie de recursos y medios para poder realizar su trabajo, contando en la medida de lo posible con el apoyo y compromiso de la Alta Dirección. (p. 71).

En el proceso propiamente dicho de gestión de riesgos se trata de definir un plan para la implantación de ciertas salvaguardas o contramedidas en el sistema informático, que permitan disminuir la probabilidad de que se materialice una amenaza, o bien reducir la vulnerabilidad del sistema o el posible impacto en

la organización, así como permitir la recuperación del sistema o la transferencia del problema a un tercero (mediante la contratación de un seguro, por ejemplo).

> De acuerdo a (Magerit, 2012), estableció que la gestión del riesgo se divide en dos tareas: (1) análisis del riesgo y (2) tratamiento de los riesgos; los cuales no son un fin en sí mismas, sino que se encajan en la actividad continua de gestión de la seguridad, el análisis de riesgos permite determinar cómo es, cuánto vale y cómo de protegido se encuentra el sistema. En coordinación con los objetivos, estrategia y política de la organización, las actividades de tratamiento de los riesgos permiten elaborar un plan de seguridad que, implantado y operado, satisfaga los objetivos propuestos con el nivel de riesgo que acepta la dirección, por lo que se deduce que el análisis de riesgos proporciona un modelo del sistema en términos de activos, amenazas y salvaguardas, y es la piedra angular para controlar todas las actividades con fundamento. La fase de tratamiento estructura las acciones que se acometen en materia de seguridad para satisfacer las necesidades detectadas por el análisis. (p. 10)

> Rosselló (2004) sostuvo: que la temática de los riesgos, tanto naturales como tecnológicos, constituye una línea de interés que ha superado con claridad la frontera del marco académico, para situarse en el ámbito del interés social, la evolución ascendente de la producción de la catástrofe, paralela sin embargo a la mejora en las técnicas estructurales de control de riesgo, ha generado una paradoja que evidencia la necesidad de comprender el proceso de producción del riesgo como un hecho complejo, dinámico y multi-causal, en el que la etiología natural o humana de los procesos se entrelazan, las causas y efectos intermedios se retroalimentan y condicionan el funcionamiento de los eventos extremos; la concurrencia en el espacio y el tiempo de acontecimientos que además se producen a distintas escalas y ritmos temporales dificultan enormemente la gestión del riesgo mediante unas

> perspectiva lineal o sectorial. El embrión de los estudios de riesgos se encuentra en un primer momento de impulso, en el análisis de las catástrofes y sus efectos iniciado en la primeras décadas del siglo xx, que impulsó proyectos de solidaridad con las víctimas de catástrofes, así como por las iniciativas de avances hacia la consolidación de una geografía de las calamidades, los resultados se concretan en la confección de un primer documento con contenido espacial, un mapa mundial de distribución geográfica de las calamidades, así como en la edición desde la Sociedad Geográfica de Ginebra en 1924. En el contexto de los años 30, las ambiciosas políticas de obras públicas constituyeron causes para la dinamización económica y la generación de empleo; tras ello subyace la idea de seguridad moderna, que da consumo con la racionalidad pragmática, y el amparo de un hombre cada vez más tecnificado, dará lugar al concepto de control del medio. (p. 103).

La filosofía que inspirara el enfoque de la problemática de riesgos hasta los años 50 es resumida por (Saurí, Ribas, Lara, y Pavón, 2010) quienes consideraron que: “si las inundaciones constituyen un fenómeno estrictamente natural, entonces deben estudiarse sus características físicas” (p. 269), y en función de estas, minimizar la ocurrencia futura de los episodios catastróficos mediante un conjunto de dispositivos tecnológico (obras hidráulicas), diseñados a partir de los datos físicos.

Luego en torno a la década de los 70 (Rosselló, 2004) nos dijo: “que se produce en el propio ámbito anglosajón una revisión crítica del modelo general de enfoque de los estudios de riesgos hasta las diversas metodología actuales” (p. 104).

> Según (Zulueta, Despaigne, y Hernández, 2009), consideraron que hay múltiples formas de tratar un riesgo: evitar las circunstancias que lo provocan, reducir las posibilidades de que ocurra, acotar sus consecuencias, compartirlo con otra organización (típicamente contratando un servicio o un seguro de cobertura), o, en última instancia, aceptando que pudiera ocurrir y previendo recursos para

> actuar cuando sea necesario. Nótese que una opción legítima es aceptar el riesgo, es frecuente oír que la seguridad absoluta no existe; en efecto, siempre hay que aceptar un riesgo que, eso sí, debe ser conocido y sometido al umbral de calidad que se requiere del servicio, es más, a veces aceptamos riesgos operacionales para acometer actividades que pueden reportarnos un beneficio que supera al riesgo, o que tenemos la obligación de afrontar. (p. 24).

1.3.2 Base teórica de la variable independiente:

Metodología de la Gestión de Riesgos de MAGERIT

El Ministerio de Hacienda y Administraciones Públicas de España se apoyó en el Consejo Superior de Administración Electrónica CSAE quien elaboró y promovió Magerit como respuesta a la percepción de que la Administración Pública (y en general toda la sociedad) depende de forma creciente de los sistemas de información para alcanzar sus objetivos, El uso de tecnologías de la información y comunicaciones (TIC) supone unos beneficios evidentes para los ciudadanos; pero también da lugar a ciertos riesgos que deben gestionarse prudentemente con medidas de seguridad que sustenten la confianza de los usuarios de los servicios; Conocer el riesgo al que están sometidos los elementos de trabajo es, simplemente, imprescindible para poder gestionarlos. En el periodo transcurrido desde la publicación de la primera versión de Magerit en 1997 hasta la fecha, el análisis de riesgos se ha venido consolidando como paso necesario para la gestión de la seguridad. Así se recoge claramente en las Directrices de la OCDE (Organismo para la cooperación y desarrollo económico) que, en su principio 6 dice: Evaluación del riesgo; Los participantes deben llevar a cabo evaluaciones de riesgo, en el esquema nacional de seguridad en el ámbito de la administración electrónica, el Capítulo II Principios Básicos, artículo 6, gestión de la seguridad basada en los riesgos dice: (1) El análisis y gestión de riesgos será parte esencial del proceso de seguridad y deberá mantenerse permanentemente actualizado, (2) La gestión de riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. La reducción de estos niveles se realizará mediante el despliegue de medidas de seguridad, que establecerá un equilibrio entre la naturaleza de los datos y los tratamientos, los riesgos a los que

estén expuestos y las medidas de seguridad.

Calder (2008) nos dijo: “La gestión de los riesgos es una piedra angular en las guías de buen gobierno, público o privado” (p. 31), donde se considera un principio fundamental que las decisiones de gobierno se fundamenten en el conocimiento de los riesgos que implican: propuesta, recopilación de los beneficios, costos, riesgos, oportunidades, y otros factores que deben tenerse en cuenta en las decisiones que se tomen, cubriendo riesgos en general y riesgos TIC en particular: esta norma establece los principios para el uso eficaz, eficiente y aceptable de las tecnologías de la información. Garantizando que sus organizaciones siguen estos principios ayudará a los directores a equilibrar riesgos y oportunidades derivados del uso de las TI.

> Younes (2004) sostuvo que la confianza es la esperanza firme que se tiene de que algo responderá a lo previsto, la confianza es un valor crítico en cualquier organización que preste servicios, las administraciones públicas son especialmente sensibles a esta valoración. Por una parte dependemos fuertemente de los sistemas de información para cumplir nuestros objetivos; pero por otra parte, no deja de ser un tema recurrente la inquietud por su seguridad, los afectados, que frecuentemente no son técnicos, se preguntan si estos sistemas merecen su confianza, confianza que se ve mermada por cada fallo y, sobre todo, cuando la inversión no se traduce en la ausencia de fallos, lo ideal es que los sistemas no fallen, pero lo cierto que se acepta convivir con sistemas que fallan, el asunto no es tanto la ausencia de incidentes como la confianza en que están bajo control, se sabe qué puede pasar y se sabe qué hacer cuando pasa, el temor a lo desconocido es el principal origen de la desconfianza y, en consecuencia, aquí se busca conocer para confiar: conocer los riesgos para poder afrontarlos y controlarlos.(p. 273).

Siguiendo la terminología de la normativa ISO 31000 (Inacal, 2011), (Magerit, 2012) estableció que: “responde a lo que se denomina proceso de gestión de los riesgos, a lo que establece la sección 4.4 (implementación de la gestión de los riesgos) dentro del marco de gestión de riesgos” (p. 7), en otras

palabras, implementa el proceso de gestión de riesgos dentro de un marco de trabajo para que los órganos de gobierno tomen decisiones teniendo en cuenta los riesgos derivados del uso de tecnologías de la información.

Visión de conjunto

Hay dos grandes tareas a realizar: (1) análisis de riesgos**,** que permite determinar qué tiene la organización y estimar lo que podría pasar. (2) tratamiento de los riesgos, que permite organizar la defensa concienzuda y prudente, defendiendo para que no pase nada malo y al tiempo estando preparados para atajar las emergencias, sobrevivir a los incidentes y seguir operando en las mejores condiciones; como nada es perfecto, según (Magerit, 2012), estableció lo siguiente: “se dice que el riesgo se reduce a un nivel residual que la dirección asume. Ambas actividades, análisis y tratamiento se combinan en el proceso denominado Gestión de Riesgos” (p. 19).

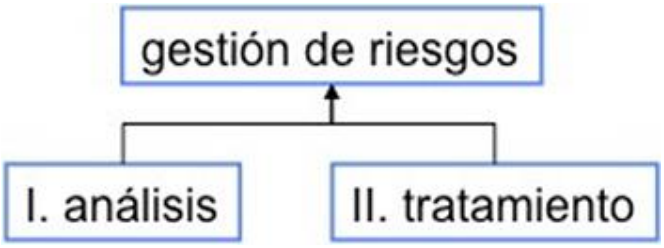


Figura 1. Gestión de riesgos
Tomado de “Metodología de Análisis y Gestión de Riesgos de los sistemas de Información,” Libro I Método, versión 3.0, por Magerit, 2012. Ministerio de Hacienda y Administraciones Públicas. Madrid, España: Autor.

> Magerit (2012) estableció que el análisis de riesgos considera los siguientes elementos: (1) activos, que son los elementos del sistema de información (o estrechamente relacionados con este) que soportan la misión de la Organización (2) amenazas, que son cosas que les pueden pasar a los activos causando un perjuicio a la Organización (3) salvaguardas (o contra medidas), que son medidas de protección desplegadas para que aquellas amenazas no causen tanto daño, con estos elementos se puede estimar: (1) el impacto: lo que podría pasar (2) el riesgo: lo que probablemente pase. (p. 21).

El análisis de riesgos permite analizar estos elementos de forma metódica

para llegar a conclusiones con fundamento y proceder a la fase de tratamiento; informalmente, se puede decir que la gestión de la seguridad de un sistema de información es la gestión de sus riesgos y que el análisis permite racionalizar dicha gestión. Formalmente, la gestión de los riesgos está estructurada de forma metódica en la norma ISO 31000 (Inacal, 2011), se propone el siguiente esquema:

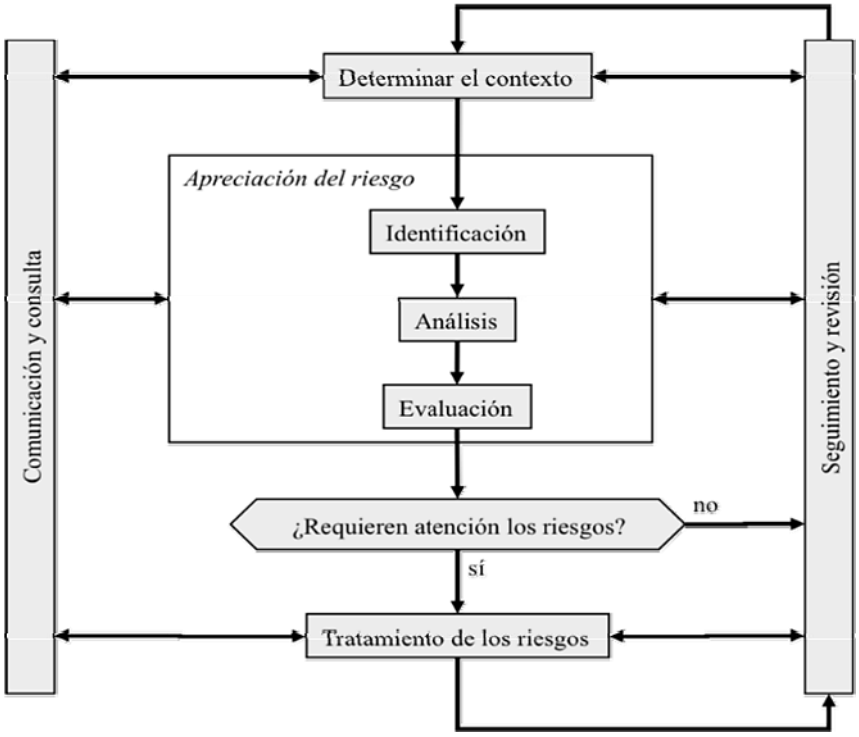


Figura 2. Proceso de gestión de riesgos
Tomado de “Gestión del riesgo. Principios y directrices,” Norma Técnica Peruana NTP - ISO 31000, por Inacal, 2011. Lima, Perú: Autor.

La determinación del contexto lleva a una determinación de los parámetros y condicionantes externos e internos que permiten encuadrar la política que se seguirá para gestionar los riesgos. Un elemento a destacar es el alcance del análisis, incluyendo obligaciones propias y obligaciones contraídas, así como las relaciones con otras organizaciones, sean para intercambio de información y servicios o proveedoras de servicios subcontratados.

La ISO 31000 (INACAL, 2011) para un mayor desarrollo de los factores que determinan el contexto propone: la identificación de los riesgos que busca una relación de los posibles puntos de peligro. Lo que se identifique será analizado en la siguiente etapa. Lo que no se identifique quedará como riesgo oculto o ignorado, el análisis de los riesgos que busca calificar los riesgos identificados,

bien cuantificando sus consecuencias (análisis cuantitativo), bien ordenando su importancia relativa (análisis cualitativo). De una u otra forma, como resultado del análisis tendremos una visión estructurada que nos permita centrarnos en lo más importante, la evaluación de los riesgos va un paso más allá del análisis técnico y traduce las consecuencias a términos de negocio. Aquí entran factores de percepción, de estrategia y de política permitiendo tomar decisiones respecto de qué riesgos se aceptan y cuáles no, así como de en qué circunstancias podemos aceptar un riesgo o trabajar en su tratamiento, el tratamiento de los riesgos recopila las actividades encaminadas a modificar la situación de riesgo, es una actividad que presenta numerosas opciones como veremos más adelante, comunicación y consulta es importante no olvidar nunca que los sistemas de información deben ser soporte de la productividad de la organización, es absurdo un sistema muy seguro pero que impide que la organización alcance sus objetivos, siempre hay que buscar un equilibrio entre seguridad y productividad y en ese equilibrio hay que contar con la colaboración de varios interlocutores: (1) los usuarios cuyas necesidades deben ser tenidas en cuenta y a los que hay que informar para que colaboren activamente en la operación del sistema dentro de los parámetros de seguridad determinados por la dirección, (2) los proveedores externos, a los que hay proporcionar instrucciones claras para poder exigirles tanto el cumplimiento de los niveles de servicio requeridos, como la gestión de los incidentes de seguridad que pudieran acaecer, (3) los órganos de gobierno para establecer canales de comunicación que consoliden la confianza de que el sistema de información responderá sin sorpresas para atender a la misión de la organización y que los incidentes serán atajados de acuerdo el plan previsto. seguimiento y revisión. Es importante no olvidar nunca que el análisis de riesgos es una actividad de despacho y que es imprescindible ver qué ocurre en la práctica y actuar en consecuencia, tanto reaccionando diligentemente a los incidentes, como mejorando continuamente nuestro conocimiento del sistema y de su entorno para mejorar el análisis y ajustarlo a la experiencia.

Método de análisis de riesgos

Conceptos paso a paso

Jácome, Pusdá y Imbaquingo (2016) concordaron que el análisis de

> riesgos es una aproximación metódica para determinar el riesgo siguiendo unos pasos pautados: (1) determinar los activos relevantes para la Organización, su interrelación y su valor, en el sentido de qué perjuicio (coste) supondría su degradación, (2) determinar a qué amenazas están expuestos aquellos activos, (3) determinar qué salvaguardas hay dispuestas y cuán eficaces son frente al riesgo, (4) estimar el impacto, definido como el daño sobre el activo derivado de la materialización de la amenaza, (5) estimar el riesgo, definido como el impacto ponderado con la tasa de ocurrencia (o expectativa de materialización) de la amenaza. Con el objeto de organizar la presentación, se introducen los conceptos de "impacto y riesgo potenciales" entre los pasos 2 y 3. Estas valoraciones son "teóricas": en el caso de que no hubiera salvaguarda alguna desplegada. Una vez obtenido este escenario teórico, se incorporan las salvaguardas del paso 3, derivando estimaciones realistas de impacto y riesgo. (p. 63).

La siguiente figura recoge este primer recorrido, cuyos pasos se detallan en las siguientes secciones:

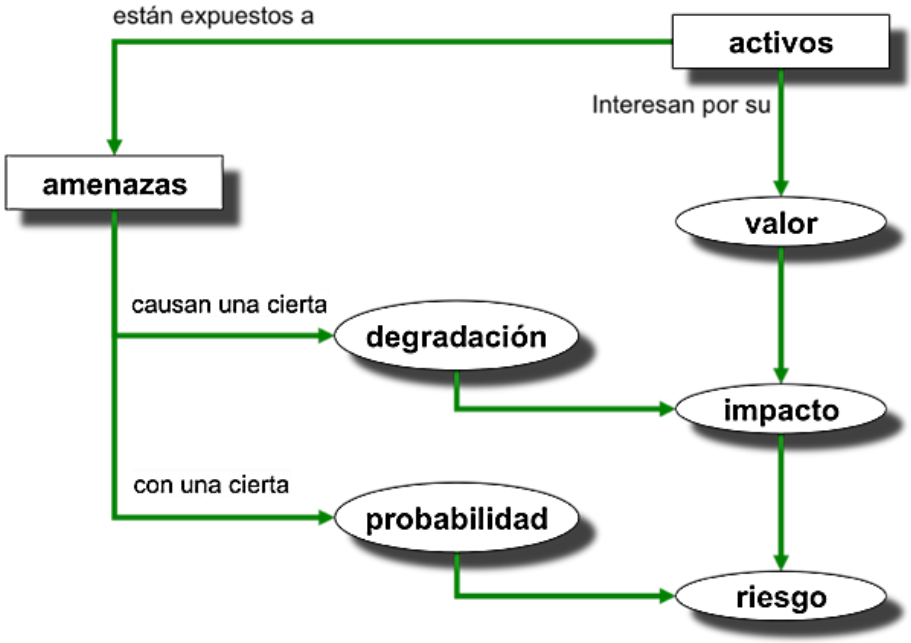


Figura 3. Elementos del análisis de riesgos potenciales
Tomado de "Gestión del riesgo. Principios y directrices," Norma Técnica Peruana NTP - ISO 31000, por Inacal, 2011. Lima, Perú: Autor.

Proceso de gestión de riesgos

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

Dentro del margen de maniobra que permita este marco, pueden aparecer consideraciones adicionales sobre la capacidad de la organización para aceptar ciertos impactos de naturaleza intangible tales como: imagen pública de cara a la sociedad (aspectos reputacionales), política interna: relaciones con los propios empleados, tales como capacidad de contratar al personal idóneo, capacidad de retener a los mejores, capacidad de soportar rotaciones de personas, capacidad de ofrecer una carrera profesional atractiva, etcétera, relaciones con los proveedores, tales como capacidad de llegar a acuerdos ventajosos a corto, medio o largo plazo, capacidad de obtener trato prioritario, etcétera, relaciones con los clientes o usuarios, tales como capacidad de retención, capacidad de incrementar la oferta, capacidad de diferenciarse frente a la competencia, relaciones con otras organizaciones, tales como capacidad de alcanzar acuerdos estratégicos, alianzas, etcétera, nuevas oportunidades de negocio, tales como formas de recuperar la inversión en seguridad, acceso a sellos o calificaciones reconocidas de seguridad.

> Magerit (2012) tomó en cuenta las consideraciones anteriores desembocando en una calificación de cada riesgo significativo, determinándose si: es crítico en el sentido de que requiere atención urgente, es grave en el sentido de que requiere atención, es apreciable en el sentido de que pueda ser objeto de estudio para su tratamiento, es asumible en el sentido de que no se van a tomar acciones para atajarlo, la opción 4, aceptación del riesgo, siempre es arriesgada y hay que tomarla con prudencia y justificación. Las

> razones que pueden llevar a esta aceptación son: (1) cuando el impacto residual es asumible, (2) cuando el riesgo residual es asumible, (3) cuando el coste de las salvaguardas oportunas es desproporcionado en comparación al impacto y riesgo residuales. La calificación de los riesgos tendrá consecuencias en las tareas subsiguientes, siendo un factor básico para establecer la prioridad relativa de las diferentes actuaciones. (p. 26).

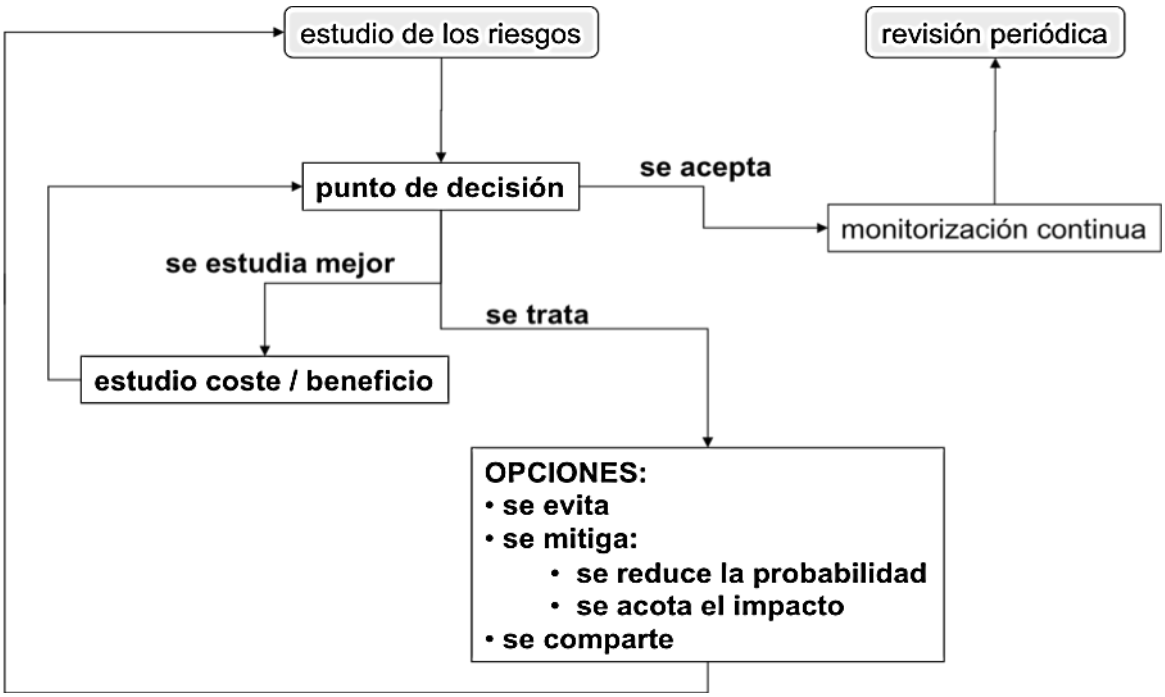


Figura 4. Decisiones de tratamiento de los riesgos
Tomado de “Metodología de Análisis y Gestión de Riesgos de los sistemas de Información,” Libro I Método, versión 3.0, por Magerit, 2012. Ministerio de Hacienda y Administraciones Públicas. Madrid, España: Autor.

Todos estos aspectos se desarrollan en las secciones siguientes:

Evaluación: interpretación de los valores de impacto y riesgo residuales

Magerit (2012) estableció: “impacto y riesgo residual son una medida del estado presente, entre la inseguridad potencial (sin salvaguarda alguna) y las medidas adecuadas que reducen impacto y riesgo a valores aceptables” (p. 29), los párrafos siguientes se refieren conjuntamente a impacto y riesgo, si el valor residual es igual al valor potencial, las salvaguardas existentes no valen para nada, típicamente no porque no haya nada hecho, sino porque hay elementos

fundamentales sin hacer. Es importante entender que un valor residual es sólo un número. Para su correcta interpretación debe venir acompañado de la relación de lo que se debería hacer y no se ha hecho; es decir, de las vulnerabilidades que presenta el sistema. Los responsables de la toma de decisiones deberán prestar cuidadosa atención a esta relación de tareas pendientes, que se denomina Informe de Insuficiencias o de vulnerabilidades.

Aceptación del riesgo

> Magerit (2012) estableció: la dirección de la organización sometida al análisis de riesgos debe determinar el nivel de impacto y riesgo aceptable. Más propiamente dicho, debe aceptar la responsabilidad de las insuficiencias. Esta decisión no es técnica. Puede ser una decisión política o gerencial o puede venir determinada por ley o por compromisos contractuales con proveedores o usuarios. Estos niveles de aceptación se pueden establecer por activo o por agregación de activos (en un determinado departamento, en un determinado servicio, en una determinada dimensión). Cualquier nivel de impacto y/o riesgo es aceptable si lo conoce y acepta formalmente la dirección. (p. 50).

Tratamiento

Magerit (2012) determinó: “la dirección puede decidir aplicar algún tratamiento al sistema de seguridad desplegado para proteger el sistema de información. Hay dos grandes opciones: reducir el riesgo residual (aceptar un menor riesgo y ampliar el riesgo residual (aceptar un mayor riesgo)” (p. 50). Para tomar una u otra decisión hay que enmarcar los riesgos soportados por el sistema de información dentro de un contexto más amplio que cubre un amplio espectro de consideraciones de las que podemos apuntar algunas sin pretender ser exhaustivos: (1) cumplimiento de obligaciones; sean legales, regulación pública o sectorial, compromisos internos, misión de la Organización, responsabilidad corporativa, etcétera, posibles beneficios derivados de una actividad que en sí entraña riesgos, (2) condicionantes técnicos, económicos, culturales, políticos, etcétera. El equilibrio con otros tipos de riesgos: comerciales, financieros,

regulatorios, medioambientales, laborales suelen darse en condiciones de riesgo residual extremo, casi la única opción es reducir el riesgo y en condiciones de riesgo residual aceptable, podemos optar entre aceptar el nivel actual o ampliar el riesgo asumido, en cualquier caso hay que mantener una monitorización continua de las circunstancias para que el riesgo formal cuadre con la experiencia real y reaccionemos ante cualquier desviación significativa.

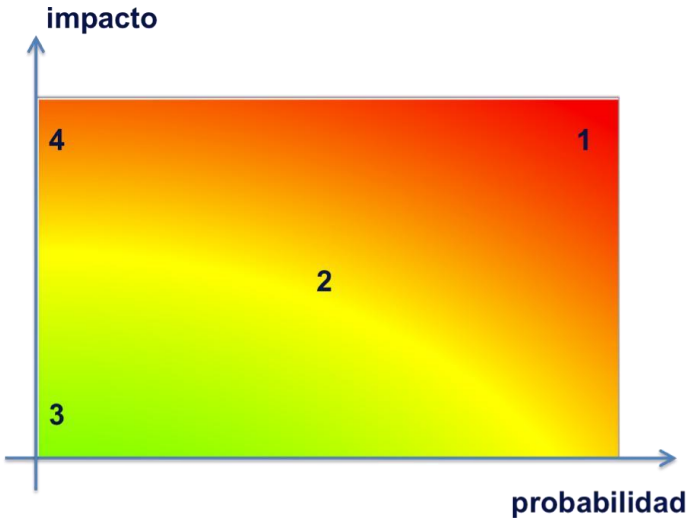


Figura 5. Zonas de riesgo
Tomado de "Metodología de Análisis y Gestión de Riesgos de los sistemas de Información," Libro I Método, versión 3.0, por Magerit, 2012. Ministerio de Hacienda y Administraciones Públicas. Madrid, España: Autor.

En condiciones de riesgo residual medio (Margerit, 2012), señaló que podemos observar otras características como las pérdidas y ganancias que pueden verse afectadas por el escenario presente, o incluso analizar el estado del sector en el que operamos para compararnos con la "norma". En términos de las zonas de riesgo que se expusieron anteriormente: zona (1) riesgos muy probables y de muy alto impacto; posiblemente nos planteemos sacarlos de esta zona, zona (2) riesgos de probabilidad relativa e impacto medio; se pueden tomar varias opciones, zona (3)– riesgos improbables y de bajo impacto; o los dejamos como están, o permitimos que suban a mayores si ello nos ofreciera alguna ventaja o beneficio en otro terreno, zona (4) riesgos improbables pero de muy alto impacto; suponen un reto de decisión pues su improbabilidad no justifica que

> se tomen medidas preventivas, pero su elevado impacto exige que tengamos algo previsto para reaccionar; es decir, hay que poner el énfasis en medidas de reacción para limitar el daño y de recuperación del desastre si ocurriera; también conviene considerar la incertidumbre del análisis, Hay veces que sospechamos las consecuencias, pero hay un amplio rango de opiniones sobre su magnitud (incertidumbre en el impacto), en otras ocasiones la incertidumbre afecta a la probabilidad, estos escenarios suelen afectar a las zonas 4 y 3, pues cuando la probabilidad es alta, normalmente adquirimos experiencia, propia o ajena, con rapidez y salimos de la incertidumbre, en cualquier caso, toda incertidumbre debe considerarse como mala y debemos hacer algo: (1) buscar formas de mejorar la previsión, típicamente indagando en foros, centros de respuesta a incidentes o expertos en la materia; (2) evitar el riesgo cambiando algún aspecto, componente o arquitectura del sistema; o (3) tener preparados sistemas de alerta temprana y procedimientos flexibles de contención, limitación y recuperación del posible incidente. A veces que estos escenarios de incertidumbre ocurren en un terreno en el que hay obligaciones de cumplimiento y la propia normativa elimina o reduce notablemente las opciones disponibles; es decir, el sistema se protege por obligación más que por certidumbre del riesgo, a la vista de estas consideraciones se tomarán las decisiones de tratamiento. (pp. 51-52).

Opciones de tratamiento del riesgo:

Eliminación

Piattini y Del Peso (2001) concordaron que: “la eliminación de la fuente de riesgo es una opción frente a un riesgo que no es aceptable, en un sistema podemos eliminar varias cosas, siempre que no afecten a la esencia de la organización” (p. 312). es extremadamente raro que podamos prescindir de la información o los servicios esenciales por cuanto constituyen la misión de la organización, cambiar estos activos supone reorientar la misión de la organización, más viable es prescindir de otros componentes no esenciales, que están presentes simple y

llanamente para implementar la misión, pero no son parte constituyente de la misma. Esta opción puede tomar diferentes formas: eliminar cierto tipo de activos, emplean otros en su lugar. Por ejemplo: cambiar de sistema operativo, de fabricante de equipos; reordenar la arquitectura del sistema (el esquema de dependencias en nuestra terminología) de forma que alteremos el valor acumulado en ciertos activos expuestos a grandes amenazas, por ejemplo: segregar redes, desdoblar equipos para atender a necesidades concretas, alejando lo más valioso de lo más expuesto, Las decisiones de eliminación de las fuentes de riesgo suponen realizar un nuevo análisis de riesgos sobre el sistema modificado.

Mitigación

Gomez (2014) nos dijo: “la mitigación del riesgo se refiere a una de dos opciones: (1) reducir la degradación causada por una amenaza (a veces se usa la expresión ‘acotar el impacto’) y (2) reducir la probabilidad de que una amenaza se materialice” (p. 74), en ambos casos lo que hay que hacer es ampliar o mejorar el conjunto de salvaguardas, en términos de madurez de las salvaguardas: subir de nivel. Algunas salvaguardas, notablemente las de tipo técnico, se traducen en el despliegue de más equipamiento que se convierte a su vez en un activo del sistema, estos nuevos activos también acumularán valor del sistema y estarán a su vez sujetos a amenazas que pueden perjudicar a los activos esenciales, hay pues que repetir el análisis de riesgos, ampliándolo con el nuevo despliegue de medios y, por supuesto, cerciorarse de que el riesgo del sistema ampliado es menor que el del sistema original; es decir, que las salvaguardas efectivamente disminuyen el estado de riesgo de la Organización.

Compartición

> Tradicionalmente (Margerit, 2012), ha hablado de ‘transferir el riesgo’. Como la transferencia puede ser parcial o total, es más general hablar de ‘compartir el riesgo’, Hay dos formas básicas de compartir riesgo: (1) riesgo cualitativo: se comparte por medio de la externalización de componentes del sistema, de forma que se reparten responsabilidades: unas técnicas para el que opera el

> componente técnico; y otras legales según el acuerdo que se establezca de prestación del servicio y (2) riesgo cuantitativo: se comparte por medio de la contratación de seguros, de forma que a cambio de una prima, el tomador reduce el impacto de las posibles amenazas y el asegurador corre con las consecuencias. Hay multitud de tipos y cláusulas de seguros para concretar el grado de responsabilidad de cada una de las partes. Cuando se comparten riesgos cambia, bien el conjunto de componentes del sistema, bien su valoración, requiriéndose un nuevo análisis del sistema resultante. (p. 92).

Financiación

Cuando se acepta un riesgo, la Organización hará bien en reservar fondos para el caso de que el riesgo se concrete y haya que responder de sus consecuencias. A veces de habla de ‘fondos de contingencia’ y también puede ser parte de los contratos de aseguramiento. Normalmente esta opción no modifica nada del sistema y nos vale el análisis de riesgos disponible. Fraume, Cristina, Ordaz y Barbat (2008)

Dimensiones de la variable independiente gestión de riesgos

Dimensión 1: Activos de información

Magerit (2012) nos explicó que un activo de información es un: “Componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización” (p. 22). Incluye: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos, en un sistema de información hay 2 cosas esenciales: la información que maneja y los servicios que presta; también se pueden identificar otros activos relevantes: datos que materializan la información, servicios auxiliares que se necesitan para poder organizar el sistema, las aplicaciones informáticas (software) que permiten manejar los datos, los equipos informáticos (hardware) y que permiten hospedar datos, aplicaciones y servicios, Los soportes de información que son dispositivos de almacenamiento de datos, el equipamiento auxiliar que complementa el

material informático, las redes de comunicaciones que permiten intercambiar datos, las instalaciones que acogen equipos informáticos y de comunicaciones, las personas que explotan u operan todos los elementos anteriormente citados. No todos los activos son de la misma especie. Dependiendo del tipo de activo, las amenazas y las salvaguardas son diferentes.

Albanese, Briozzo, Argañaraz y Vigier (2013) concordaron que los activos esenciales son: la información y los servicios prestados; pero estos activos dependen de otros activos más prosaicos como pueden ser los equipos, las comunicaciones, las instalaciones y las frecuentemente olvidadas personas que trabajan con aquellos. De manera que los activos vienen a formar árboles o grafos de dependencias donde la seguridad de los activos que se encuentran más arriba en la estructura o 'superiores' depende de los activos que se encuentran más abajo o 'inferiores'. Estas estructuras reflejan de arriba hacia abajo las dependencias, mientas que de abajo hacia arriba la propagación del daño caso de materializarse las amenazas. Por ello aparece como importante el concepto de "dependencias entre activos" o la medida en que un activo superior se vería afectado por un incidente de seguridad en un activo inferior, se dice que un "activo superior" depende de otro "activo inferior" cuando las necesidades de seguridad del superior se reflejan en las necesidades de seguridad del inferior; O, dicho en otras palabras, cuando la materialización de una amenaza en el activo inferior tiene como consecuencia un perjuicio sobre el activo superior.

Galeano, Escobar, Cuartas, y Botero (2015) nos dijeron que informalmente puede interpretarse que los activos inferiores son los pilares en los que se apoya la seguridad de los activos superiores. Aunque en cada caso hay que adaptarse a la Organización objeto del análisis, con frecuencia se puede estructurar el conjunto de activos en capas, donde las capas superiores dependen de las inferiores: (1) activos esenciales, (2) información que se maneja, (3) servicios prestados, (4) servicios internos que estructuran ordenadamente el sistema de información, (5) el equipamiento informático, (6) aplicaciones (software), (7) equipos informáticos (hardware), (8) comunicaciones, (9) soportes de información: discos, cintas, etcétera, (10) el entorno: activos que se precisan para garantizar las siguientes capas, (11) equipamiento y suministros: energía, climatización,

etcétera, (12) mobiliario, (13) los servicios subcontratados a terceros, (14) las instalaciones físicas, (15) el personal, (16) usuarios, (17) operadores y administradores, (18) desarrolladores.

Dimensión 2: Amenazas

> Magerit (2012) determinó que la causa potencial de un incidente que puede ocasionar daños a un sistema de información o a una organización, se identifican de la siguiente manera: (1) De origen natural, hay accidentes naturales (terremotos, inundaciones, etcétera), ante esos avatares el sistema de información es víctima pasiva, pero de todas formas tendremos en cuenta lo que puede suceder, (2) Del entorno (de origen industrial) hay desastres industriales (contaminación, fallos eléctricos, etcétera) ante los cuales el sistema de información es víctima pasiva; pero no por ser pasivos hay que permanecer indefensos, (3) Defectos de las aplicaciones, hay problemas que nacen directamente en el equipamiento propio por defectos en su diseño o en su implementación, con consecuencias potencialmente negativas sobre el sistema. Frecuentemente se denominan vulnerabilidades técnicas o, simplemente, 'vulnerabilidades, (4) Causadas por las personas de forma accidental, las personas con acceso al sistema de información pueden ser causa de problemas no intencionados, típicamente por error o por omisión, (5) causadas por las personas de forma deliberada, las personas con acceso al sistema de información pueden ser causa de problemas intencionados: ataques deliberados; bien con ánimo de beneficiarse indebidamente, bien con ánimo de causar daños y perjuicios a los legítimos propietarios. No todas las amenazas afectan a todos los activos, sino que hay una cierta relación entre el tipo de activo y lo que le podría ocurrir. (pp. 27-28).

Freitas (2009) dijo: cuando un activo es víctima de una amenaza, no se ve afectado en todas sus dimensiones, ni en la misma cuantía, una vez determinado que una amenaza puede perjudicar a un activo, hay que valorar su influencia en el valor del activo, en dos sentidos: degradación: cuán perjudicado resultaría el

valor del activo y probabilidad: cuán probable o improbable es que se materialice la amenaza, la degradación mide el daño causado por un incidente en el supuesto de que ocurriera, la degradación se suele caracterizar como una fracción del valor del activo y así aparecen expresiones como que un activo se ha visto totalmente degradado, o degradado en una pequeña fracción. Cuando las amenazas no son intencionales, probablemente baste conocer la fracción físicamente perjudicada de un activo para calcular la pérdida proporcional de valor que se pierde, pero cuando la amenaza es intencional, no se puede pensar en proporcionalidad alguna pues el atacante puede causar muchísimo daño de forma selectiva.

Dimensión 3: Impacto potencial

Magerit (2012) definió de la siguiente manera a esta dimensión: “se denomina impacto a la medida del daño sobre el activo derivado de la materialización de una amenaza, conociendo el valor de los activos y la degradación que causan las amenazas” (p. 29), es directo derivar el impacto que estas tendrían sobre el sistema, la única consideración que queda hacer es relativa a las dependencias entre activos, es frecuente que el valor del sistema se centre en la información que maneja y los servicios que presta; pero las amenazas suelen materializarse en los medios. Para enlazar unos con otros recurriremos al grafo de dependencias: (1) impacto acumulado, es el calculado sobre un activo teniendo en cuenta su valor acumulado (el propio mas el acumulado de los activos que dependen de él) y las amenazas a que está expuesto, el impacto acumulado se calcula para cada activo, por cada amenaza y en cada dimensión de valoración, siendo una función del valor acumulado y de la degradación causada. El impacto es tanto mayor cuanto mayor es el valor propio o acumulado sobre un activo o cuanto mayor sea la degradación del activo atacado, al calcularse sobre los activos que soportan el peso del sistema de información, permite determinar las salvaguardas de que hay que dotar a los medios de trabajo: protección de los equipos, copias de respaldo, etcétera, (2) impacto repercutido, es el calculado sobre un activo teniendo en cuenta su valor propio y las amenazas a que están expuestos los activos de los que depende el impacto repercutido se calcula para cada activo, por cada amenaza y en cada dimensión de valoración, siendo una función del valor propio y de la degradación causada. El impacto es tanto mayor

cuanto mayor es el valor propio de un activo, cuanto mayor sea la degradación del activo atacado, cuanto mayor sea la dependencia del activo atacado. El impacto repercutido, al calcularse sobre los activos que tienen valor propio, permite determinar las consecuencias de las incidencias técnicas sobre la misión del sistema de información, es pues una presentación gerencial que ayuda a tomar una de las decisiones críticas de un análisis de riesgos: aceptar un cierto nivel de riesgo.

Dimensión 4: Riesgo potencial

> De acuerdo a Margerit (2012), definió riesgo potencial a la medida del daño probable sobre un sistema. Conociendo el impacto de las amenazas sobre los activos, es directo derivar el riesgo sin más que tener en cuenta la probabilidad de ocurrencia, aquí se define : (1) riesgo acumulado, que es el calculado sobre un activo teniendo en cuenta el impacto acumulado sobre un activo debido a una amenaza y la probabilidad de la amenaza, el riesgo acumulado se calcula para cada activo, por cada amenaza y en cada dimensión de valoración, siendo una función del valor acumulado, la degradación causada y la probabilidad de la amenaza, el riesgo acumulado, al calcularse sobre los activos que soportan el peso del sistema de información, permite determinar las salvaguardas de que hay que dotar a los medios de trabajo: protección de los equipos, copias de respaldo, etcétera, (2) riesgo repercutido, es el calculado sobre un activo teniendo en cuenta el impacto repercutido sobre un activo debido a una amenaza y la probabilidad de la amenaza, el riesgo repercutido se calcula para cada activo, por cada amenaza y en cada dimensión de valoración, siendo una función del valor propio, la degradación causada y la probabilidad de la amenaza. El riesgo repercutido, al calcularse sobre los activos que tienen valor propio, permite determinar las consecuencias de las incidencias técnicas sobre la misión del sistema de información. Es pues una presentación gerencial que ayuda a tomar una de las decisiones críticas de un análisis de riesgos: aceptar un cierto nivel de riesgo. (p. 30).

Abril, Pulido y Bohada (2017) establecieron que el riesgo sobre un activo tendría una amenaza en una cierta dimensión. Estos riesgos singulares pueden agregarse bajo ciertas condiciones: (1) puede agregarse el riesgo repercutido sobre diferentes activos, (2) puede agregarse el impacto acumulado sobre activos que no sean dependientes entre sí, y no hereden valor de un activo superior común, (3) no debe agregarse el riesgo acumulado sobre activos que no sean independientes, pues ello supondría sobre ponderar el riesgo al incluir varias veces el valor acumulado de activos superiores, (4) puede agregarse el riesgo de diferentes amenazas sobre un mismo activo, aunque conviene considerar en qué medida las diferentes amenazas son independientes y pueden ser concurrentes, (5) puede agregarse el riesgo de una amenaza en diferentes dimensiones.

Dimensión 5: Salvaguardas

Magerit (2012) definió de la siguiente manera a esta dimensión: en los pasos anteriores no se han tomado en consideración las salvaguardas desplegadas, se miden, por tanto, los impactos y riesgos a que estarían expuestos los activos si no se protegieran en absoluto" (p. 30), en la práctica no es frecuente encontrar sistemas desprotegidos: las medidas citadas indican lo que ocurriría si se retiraran las salvaguardas presentes. Se definen las salvaguardas o contra medidas como aquellos procedimientos o mecanismos tecnológicos que reducen el riesgo, hay amenazas que se conjuran simplemente organizándose adecuadamente, otras requieres elementos técnicos (programas o equipos), otras seguridades físicas y, por último, está la política de personal. Ante el amplio abanico de posibles salvaguardas a considerar, es necesario hacer una criba inicial para quedarnos con aquellas que son relevantes para lo que hay que proteger, en esta criba se deben tener en cuenta los siguientes aspectos: (1) tipo de activos a proteger, pues cada tipo se protege de una forma específica, (2) dimensión o dimensiones de seguridad que requieren protección, (3) amenazas de las que necesitamos protegernos, (4) si existen salvaguardas alternativas, además, es prudente establecer un principio de proporcionalidad y tener en cuenta: el mayor o menor valor propio o acumulado sobre un activo, centrándonos en lo más valioso y obviando lo irrelevante, la mayor o menor probabilidad de que una amenaza ocurra, centrándonos en los riesgos más importantes, la cobertura

del riesgo que proporcionan salvaguardas alternativas

Jiménez, Vicente, y Mateos (2015) concordaron que esto lleva a dos tipos de declaraciones para excluir una cierta salvaguarda del conjunto de las que conviene analizar: (1) no aplica se dice cuando una salvaguarda no es de aplicación porque técnicamente no es adecuada al tipo de activos a proteger, no protege la dimensión necesaria o no protege frente a la amenaza en consideración, (2) no se justifica se dice cuando la salvaguarda aplica, pero es desproporcionada al riesgo que tenemos que proteger como resultado de estas consideraciones dispondremos de una “declaración de aplicabilidad” o relación de salvaguardas que deben ser analizadas como componentes nuestro sistema de protección. Las salvaguardas entran en el cálculo del riesgo de dos formas: (1) reduciendo la probabilidad de las amenazas, se llaman salvaguardas preventivas, las ideales llegan a impedir completamente que la amenaza se materialice y (2) limitando el daño causado, hay salvaguardas que directamente limitan la posible degradación, mientras que otras permiten detectar inmediatamente el ataque para frenar que la degradación avance, incluso algunas salvaguardas se limitan a permitir la pronta recuperación del sistema cuando la amenaza lo destruye. En cualquiera de las versiones, la amenaza se materializa; pero las consecuencias se limitan.

Importancia de la gestión de riesgos en el programa de desarrollo agrario rural

Una buena gestión del riesgo garantiza una continuidad operativa (Agrorural, 2017) sostenida en el tiempo y siempre acorde con la renovación tecnológica frente a los cambios tantos externos como internos. Debido a ello, los ingenieros en sistemas y el personal responsable de las tecnologías de la información en las organizaciones, deben tener conciencia sobre la existencia de los riesgos relacionados, y administrarlos adecuadamente. La gestión de riesgos de TI requiere del conocimiento de los principios y conceptos que la sustentan y de comprender las acciones que se deben realizar para que los objetivos organizacionales sean alcanzados dentro del marco normado por la Secretaria de gobierno digital de la PCM (Indecopi, 2014)

Hay varias aproximaciones al problema de analizar los riesgos soportados por los sistemas TIC: guías informales, aproximaciones metódicas y herramientas de soporte. Todas buscan objetivar el análisis de riesgos para saber cuán seguros (o inseguros) son los sistemas y no llamarse a engaño. El gran reto de todas estas aproximaciones es la complejidad del problema al que se enfrentan; complejidad en el sentido de que hay muchos elementos que considerar y que, si no se es riguroso, las conclusiones serán de poco fiar. Es por ello que la presente investigación persigue una aproximación metódica que no deje lugar a la improvisación, ni dependa de la arbitrariedad del analista. Se persigue los siguientes objetivos: (1) concienciar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos, (2) ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC), (3) ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control Indirectos, (4) preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso.

1.3.3 Conceptualización variable dependiente: Seguridad de la información

Piattini y Del Peso (2001) indicó que a la seguridad de la informacion como la doctrina que trata de los riesgos informaticos o creados por la informatica, por tanto, el nivel de seguridad informatica en una entidad es un objetivo a evaluar y esta directamente relacionado con la calidad y eficacia de un conjunto de acciones y medidas destinadas a proteger y preservar la informacion de la entidad y sus medios de proceso. Resumiendo , la informatica crea unos riesgos informaticos de los que hay que proteger y preservar a la entidad con un entramado de contramedidas, y la calidad y la eficacia de las mismas es el objetivo a evaluar para poder identificar asi sus puntos debiles y mejorarlos.. Esta es una de las funciones de la seguridad informatica, donde se debe profundizar mas en ese entramado de contramedidas para ver que papel tienen las metodologias y los CISO (director de seguridad de la informacion) en los mismos, para explicar esta medida diremos que cualquier contramedida nace de la composicion de varios factores: (1) estandares publicas, (2) funciones, procedimientos y planes, (3) informatica, usuarios, (4) hardware y software.

Gomez (2014) señaló que “la seguridad de la informacion es cualquier medida que impida la ejecución de operaciones no autorizadas sobre un sistema o red informática” (p. 41), cuyos efectos puedan conllevar daños sobre la información, comprometer su confidencialidad, autenticidad o integridad, disminuir el rendimiento de los equipos o bloquear el acceso de usuarios autorizados al sistema, Asimismo, es necesario considerar otros aspectos o cuestiones relacionados cuando se habla de Seguridad Informática: (1) cumplimiento de las regulaciones legales aplicables a cada sector o tipo de organización, dependiendo del marco legal de cada país, (2) control en el acceso a los servicios ofrecidos y la información guardada por un sistema informático, (3) control en el acceso y utilización de ficheros protegidos por la ley: contenidos digitales con derechos de autor, ficheros con datos de carácter personal, etcétera, (4) Identificación de los autores de la información o de los mensajes, (5) registro del uso de los servicios de un sistema informático, etcetera.

> Magerit (2012) aseguró que la seguridad de la información es la capacidad de las redes o de los sistemas de información para resistir, con un determinado nivel de confianza, los accidentes o acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos y de los servicios que dichas redes y sistemas ofrecen o hacen accesibles. Asi mismo nos dice que el mejor plan de seguridad se vería seriamente hipotecado sin una colaboración activa de las personas involucradas en el sistema de información, especialmente si la actitud es negativa, contraria a las medidas, o tienen la percepción de pasarse el día “luchando contra las absurdas medidas de seguridad”, es por ello que se requiere la creación de una “cultura de seguridad” que, emanando de la alta dirección, conciencie a todos los involucrados de su necesidad y pertinencia. Son tres los pilares fundamentales para la creación de esta cultura: una política de seguridad corporativa que se entienda (escrita para los que no son expertos en la materia), que se difunda y que se mantenga al día. Una normativa se seguridad

> que, entrando en áreas específicas de actividad, aclare la postura de la Organización; es decir, defina lo que es uso correcto y lo que es incumplimiento. Una formación continua a todos los niveles, recordando las cautelas rutinarias y las actividades especializadas, según la responsabilidad adscrita a cada puesto de trabajo. (p. 75).

La seguridad de la información no es una propiedad funcional de un sistema de información, sino más bien una propiedad emergente, a lo largo de los años, la percepción de la seguridad de la información ha ido cambiando hasta llegar a nuestros días, nació ligada a los entornos militares, diplomáticos y gubernamentales, a nivel empresarial comenzó siendo un lujo, algo que estaba bien pero no era necesario; seguidamente paso a estar de moda, e incluso, a ser una recomendación útil y deseable, percibiéndose como un gasto necesario para poder llevar a cabo los negocios, posteriormente se consideró como una obligación para que las empresas no queden desprotegidas, desde el punto de vista legal, frente a leyes ya reglamentos tales como la ley de la propiedad intelectual e industrial. En la actualidad, la seguridad de la información se ha convertido en un elemento integral de la capacidad de una organización para que esta sea competitiva, es por ello, un activo estratégico que no puede estar separado del núcleo de todo negocio u organización, percibiéndose como una de las mejores inversiones para el futuro de la empresa. En el ámbito de los contrasentidos, actualmente podemos encontrar algunas empresas que afirman que les preocupa mucho la seguridad de la información, pero que no cuentan con personal formado para la seguridad, no disponen de un presupuesto explicito para tal fin o que no investigan los incidentes de seguridad, o bien creen que su negocio carece de interés para cualquier potencial atacante, obviamente esto está ayudando a que atacantes utilicen a estas empresas como zombies para sus fines lucrativos y delictivos. (Bertolín, 2008).

1.3.4 Base teórica de la variable dependiente: Seguridad de la Información

Gómez (2014) nos dijo: “nadie cuestiona hoy en día la importancia adquirida por la seguridad informática y la protección de datos para cualquier organización, ya sea ésta una empresa o una institución dependiente de una administración pública” (p. 34), la progresiva informatización de los procesos

administrativos y de negocio, el despliegue de redes privadas de datos y el desarrollo de nuevos servicios on-line a través de Internet son algunos de los factores que explican la creciente preocupación por mejorar la seguridad en los sistemas de información y en el uso de los servicios de las redes de ordenadores. La información constituye un recurso que en muchos casos no se valora adecuadamente por su intangibilidad (situación que no se produce con los equipos informáticos, la documentación impresa o las aplicaciones) y, además, las medidas de seguridad no contribuyen a mejorar la productividad de los sistemas y redes informáticas, sino, más bien, todo lo contrario, ya que pueden reducir el rendimiento de los equipos y las aplicaciones (los sistemas criptográficos, por ejemplo, consumen mayores recursos computacionales y ancho de banda en las conexiones a Internet), por lo que las organizaciones son reticentes a dedicar recursos a esta tarea. Asimismo, con la proliferación de las redes de ordenadores la información de las empresas ha pasado de concentrarse en los grandes sistemas (sistemas centralizados) a distribuirse por los ordenadores y servidores ubicados en los distintos departamentos y grupos de trabajo repartidos por todas las sedes y delegaciones de la organización.

Por este motivo, en la actualidad muchas organizaciones no conocen la información que se guarda en los puestos de trabajo (generalmente, ordenadores personales de la propia organización), ni los riesgos presentes que se derivan de posibles ataques informáticos o de desastres físicos, ni cómo la propia organización utiliza esa información, otro aspecto importante, que muchas veces se olvida, es que, según varios estudios publicados, más del 75% de los problemas inherentes a la seguridad informática se producen por fallos de los equipos o por un mal uso por parte del personal de la propia organización. Por este motivo, la implantación de un sistema de gestión de seguridad de la Información debería considerar el factor humano como uno de sus elementos clave, contemplando aspectos como la adecuada formación y sensibilización de los empleados, la implicación de los responsables y directivos, la aprobación de un reglamento Interno sobre el uso de la Informática e Internet en la organización, etcétera, además el entorno legal que ha entrado en vigor en estos últimos años en países como España sobre protección de datos

de carácter personal y prestación de servicios de la sociedad de la información, plantea nuevos retos técnicos y organizativos para los retos para los responsables de la seguridad de la información.

Así, en España la Ley Orgánica 15/1999, de 13 de diciembre, sobre Protección de datos de carácter personal (LOPD) obliga a la implantación de importantes medidas de seguridad informática a las organizaciones (tanto públicas como privadas) que hayan creado ficheros con datos personales, en otros países como Estados Unidos debemos tener en cuenta otras obligaciones relacionadas con la seguridad Informática previstas por leyes como la Sarbanes-Oxley.

En esta investigación se pretende abordar la segundad contemplando tantos los aspectos técnicos, como los factores humanos y organizativos, así corno el cumplimiento del entorno legal.

Que se entiende por seguridad de la información

> Macau (2004) contempló que muchas de las actividades que se realizan de forma cotidiana en los países desarrollados dependen en mayor o menor medida de sistemas y de redes informáticas. El espectacular crecimiento de Internet y de los servicios telemáticos (comercio electrónico, servicios multimedia de banda ancha, administración electrónica, herramientas de comunicación como el correo electrónico o la videoconferencia) ha contribuido a popularizar aún más, si cabe, el uso de la informática y de las redes de ordenadores, hasta el punto de que en la actualidad no se circunscriben al ámbito laboral y profesional, sino que incluso se han convertido en un elemento cotidiano en muchos hogares, con un creciente impacto en las propias actividades de comunicación y de ocio de los ciudadanos. Por otra parte, servicios críticos para una sociedad moderna, como podrían ser los servicios financieros, el control de la producción y suministro eléctrico (centrales eléctricas, redes de distribución y transformación), los medios de transporte (control de tráfico aéreo, control de vías terrestres y

> marítimas), la sanidad (historial clínico informatizado, telemedicina), las redes de abastecimiento (agua, gas y saneamiento) o la propia administración pública están soportados en su práctica totalidad por sistemas y redes informáticas, hasta el punto de que en muchos de ellos se han eliminado o reducido de forma drástica los papeles y los procesos manuales.(p. 7).
>
> Delgado y Marín (2000) estableció que en las propias empresas, la creciente complejidad de las relaciones con el entorno y el elevado número de transacciones realizadas corno parte de su actividad han propiciado el soporte automatizado e informatizado de muchos de sus procesos, situación que se ha acelerado con la implantación de los ERP, o paquetes software de gestión integral, por todo ello, en la actualidad las actividades cotidianas de las empresas y de las distintas administraciones públicas e, incluso, las de muchas otras instituciones y organismos, así como las de los propios ciudadanos, requieren del correcto funcionamiento de los sistemas y redes informáticas que las soportan y, en especial, de su seguridad, de ahí la gran importancia que se debería conceder a todos los aspectos relacionados con la seguridad informática en una organización, La proliferación de los virus y códigos malignos y su rápida distribución a través de redes como Internet, así como los miles de ataques e incidentes de seguridad que se producen todos los años han contribuido a despertar un mayor interés por esta cuestión. (p. 37).

Desde un punto de vista más amplio, en la norma ISO/IEC 17799 (Indecopi, 2014) se define la seguridad de la información como la preservación de su confidencialidad, su integridad y su disponibilidad.

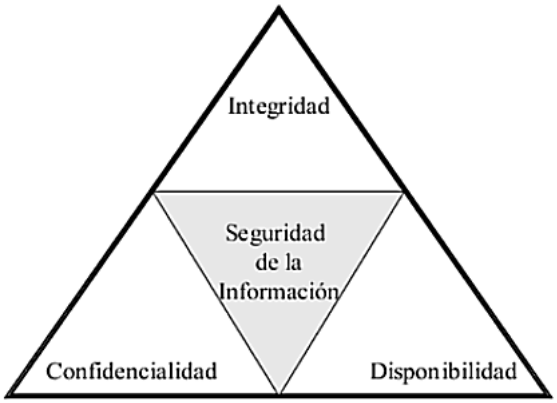


Figura 6. Seguridad de la información
Tomado de “Tecnología de la Información. Técnicas de seguridad. Sistemas de Gestión de seguridad de la información. Requisitos,” Norma Técnica Peruana NTP - ISO 27001: 2014, por Indecopi, 2014. Lima, Perú: Autor

Debemos tener en cuenta que la seguridad de un sistema informático dependerá de diversos factores, entre los que podríamos destacar los siguientes: (1) la sensibilización de los directivos y responsables de la organización, que deben ser conscientes de la necesidad de destinar recursos a esta función, (2) los conocimientos, capacidades e implicación de los responsables del sistema informático: dominio de la tecnología utilizada en el sistema informático y conocimiento sobre las posibles amenazas y los tipos de ataques, (3) la mentalización, formación y asunción de responsabilidades de todos los usuarios del sistema, (4) la correcta instalación, configuración y mantenimiento de los equipos, (5) la limitación en la asignación de los permisos y privilegios de los usuarios, (6) el soporte de los fabricantes de hardware y software, con la publicación de parches y actualizaciones de sus productos que permitan corregir los fallos y problemas relacionados con la seguridad, (7) contemplar no sólo la seguridad frente a las amenazas del exterior, sino también las amenazas procedentes del interior de la organización, aplicando además el principio de "Defensa en Profundidad”, (8) la adaptación de los objetivos de seguridad y de las actividades a realizar a las necesidades reales de la organización, en este sentido, se deberían evitar políticas y procedimientos genéricos, definidos para tratar de cumplir los requisitos impuestos por otros organismos. Podernos afirmar que hoy en día uno de los principios de las buenas prácticas de la gestión corporativa es el de la seguridad de la información, siendo responsabilidad de la alta dirección

el poner los recursos y medios necesarios para la implantación de un adecuado sistema de gestión de la seguridad de la información en el conjunto de la organización (Indecopi, 2014).

Objetivos de la seguridad de información

> Entre los principales objetivos de la seguridad informática podríamos destacar los siguientes: (1) Minimizar y gestionar los riesgos y detectar los posibles problemas y amenazas a la seguridad, (2) Garantizar la adecuada utilización de los recursos y de las aplicaciones del sistema, (3) Limitar las pérdidas y conseguir la adecuada recuperación del sistema en caso de un incidente de seguridad, (4) cumplir con el marco legal y con los requisitos impuestos por los clientes en sus contratos. Para cumplir con estos objetivos una organización debe contemplar cuatro planos de actuación: (1) Técnico**,** tanto a nivel físico como a nivel lógico, (2) Legal**,** algunos países obligan por Ley a que en determinados sectores se implanten una serie de medidas de seguridad (sector de servicios financieros y sector sanitario en Estados Unidos, protección de datos personales en todos los estados miembros de la Unión Europea, etcétera), (3) Humano**,** sensibilización y formación de empleados y directivos, definición de funciones y obligaciones del personal, (4) Organizativo**,** definición e implantación de políticas de seguridad, planes, normas, procedimientos y buenas prácticas de actuación. (Gómez, 2014, p. 64).

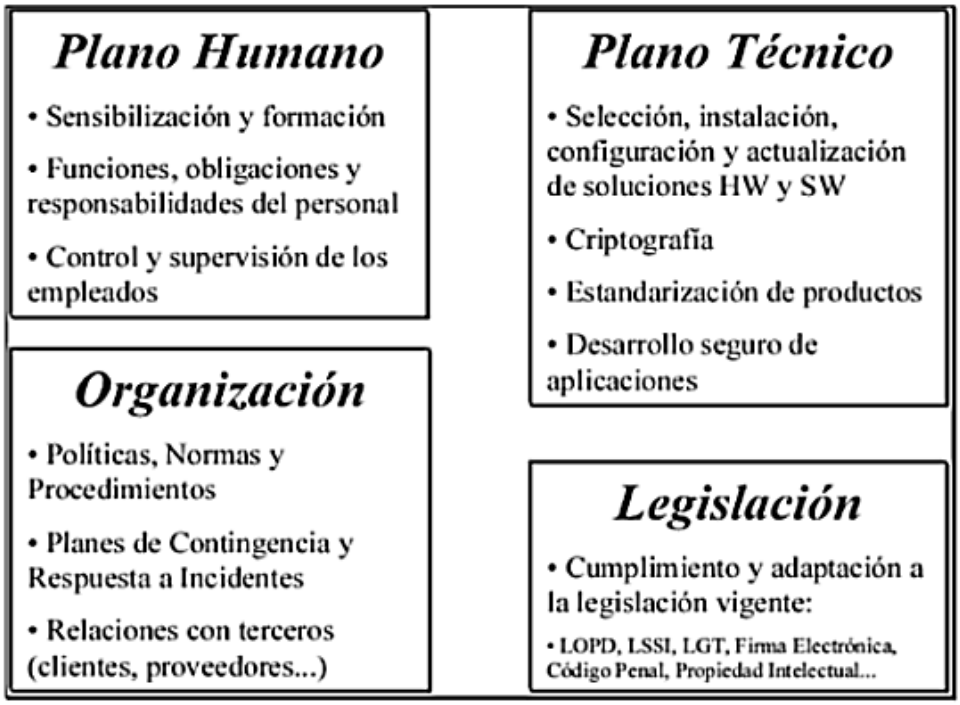


Figura 7. Planos de actuación en la seguridad de la información
Tomado de “Enciclopedia de la Seguridad Informática,” RAMA (Segunda ed.), por Gómez, 2014. Madrid, España: Autor.

Una organización debe entender la seguridad Informática como un proceso y no como un producto que se pueda "comprar" o "instalar". Se trata, por lo tanto, de un ciclo iterativo, en el que se incluyen actividades como la valoración de riesgos, prevención, detección y respuesta ante incidentes de seguridad, por otra parte, la problemática asociada a la adecuada gestión de la seguridad en una organización del siglo XXI se ve condicionada por distintos factores y características del propio sistema informático y de su entorno. Así, sería necesario contemplar cuestiones como el nivel de centralización/descentralización del sistema, la necesidad de garantizar un funcionamiento continuado del sistema, el nivel de sensibilidad de los datos y de los recursos, la existencia de un entorno potencialmente hostil (conexiones a redes abiertas como Internet) o el cumplimiento del marco legal vigente (Protección de Datos Personales, Protección de la Propiedad Intelectual, Delitos Informáticos) y de la certificación basada en una serie de estándares internacionales (BS 7799-2, ISO 27001) o nacionales. (Indecopi, 2014).

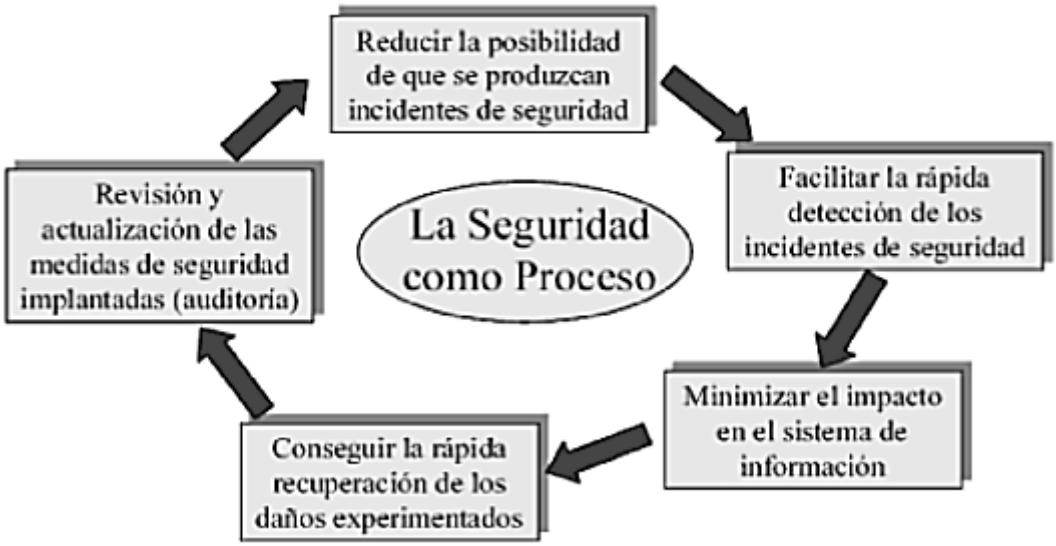


Figura 8. Seguridad informática como proceso y no como producto
Tomado de "Enciclopedia de la Seguridad Informática," RAMA (Segunda ed.), por Gómez, 2014. Madrid, España: Autor.

Servicios de seguridad de información

Para poder alcanzar los objetivos descritos en el apartado anterior, dentro del proceso de gestión de la seguridad informática es necesario contemplar una serie de servicios o funciones de seguridad de la información:

Confidencialidad

> Gómez (2014) señaló que mediante este servicio o función de seguridad se garantiza que cada mensaje transmitido o almacenado en un sistema informático sólo podrá ser leído por su legítimo destinatario. Si dicho mensaje cae en manos de terceras personas, éstas no podrán acceder al contenido del mensaje original; Por lo tanto, este servicio pretende garantizar la confidencialidad de los datos almacenados en un equipo, de los datos guardados en dispositivos de backup y/o de los datos transmitidos a través de redes de comunicaciones. (p. 47).

Autenticación

> Gómez (2012) indicó que la autenticación garantiza que la identidad del creador de un mensaje o documento es legítima, es

> decir, gracias a esta función, el destinatario de un mensaje podrá estar seguro de que su creador es la persona que figura como remitente de dicho mensaje. Asimismo, también podemos hablar de la autenticidad de un equipo que se conecta a una red o intenta acceder a un determinado servicio. En este caso, la autenticación puede ser unilateral, cuando sólo se garantiza la identidad del equipo (usuario o terminal que se intenta conectar a la red) o mutua, en el caso de que la red o el servidor también se autentica de cara al equipo, usuario o terminal que establece la conexión. (p.48).

Integridad

Gómez (2014) nos dijo que: “la función de integridad se encarga de garantizar que un mensaje o fichero no ha sido modificado desde su creación o durante su transmisión a través de una red informática” (p. 49). De este modo, es posible detectar si se ha añadido o eliminado algún dato en un mensaje o fichero almacenado, procesado o transmitido por un sistema o red informática. La integridad afecta directamente al correcto desempeño de las funciones de una Organización.

No repudiación

> Según (Gómez, 2014) estableció que el objeto del servicio de seguridad consiste en implementar un mecanismo probatorio que permita demostrar la autoría y envío de un determinado mensaje, de tal modo que el usuario que lo ha creado y enviado a través del sistema no pueda posteriormente negar esta circunstancia, situación que también se aplica al destinatario del envío. Éste es un aspecto de especial importancia en las transacciones comerciales y que permite proporcionar a los compradores y vendedores una seguridad jurídica que va a estar soportada por este servicio. En un sistema informático, por lo tanto, se puede distinguir entre la no repudiación de origen y la no repudiación de destino. (p.49).

Disponibilidad

Gómez (2012) nos dijo también: “la disponibilidad del sistema informático también es una cuestión de especial importancia para garantizar el cumplimiento de sus objetivos, ya que se debe diseñar un sistema lo suficientemente robusto frente a ataques e interferencias como para garantizar su correcto funcionamiento”, (p. 50), de manera que pueda estar permanentemente a disposición de los usuarios que deseen acceder. La carencia de disponibilidad supone una interrupción del servicio. La disponibilidad afecta directamente a la productividad de las organizaciones, debemos tener en cuenta que de nada sirven los demás servicios de seguridad si el sistema informático no se encuentra disponible para que pueda ser utilizado por sus legítimos usuarios y propietarios.

En un sistema informático se puede recurrir a la implantación de distintas técnicas y mecanismos de seguridad para poder ofrecer los servicios de seguridad que se han descrito anteriormente: identificación de usuarios y política de contraseñas, control lógico de acceso a los recursos, copias de seguridad, centros de respaldo, cifrado de las transmisiones, huella digital de mensajes, sellado temporal de mensajes, utilización de la firma electrónica, protocolos criptográficos, análisis y filtrado del tráfico (cortafuegos), servidores proxy, sistema de detección de intrusiones (IDS), antivirus, etcétera.

Gestión de la seguridad de la información

Para gestionar la seguridad de la información es preciso contemplar toda una serie de tareas y de procedimientos que permitan garantizar los niveles de seguridad exigibles en una organización, teniendo en cuenta que los riesgos no se pueden eliminar totalmente, pero sí se pueden gestionar. En este sentido, conviene destacar que en la práctica resulta imposible alcanzar la seguridad al 100% y, por este motivo, algunos expertos prefieren hablar de la fiabilidad del sistema informático, entendiendo como tal la probabilidad de que el sistema se comporte tal y como se espera de él. En palabras del experto Gene Spafford, (Gómez, 2014), estableció: "el único sistema verdaderamente seguro es aquel que se encuentra apagado, encerrado en una caja fuerte de titanio, enterrado en un bloque de hormigón, rodeado de gas nervioso y vigilado por

guardias armados y muy bien pagados. Incluso entonces, yo no apostaría mi vida por ello". (p.63).

> Gómez (2014) por otra parte, estableció que las políticas de gestión Información están constituidas por el conjunto de la seguridad de la normas reguladoras, procedimientos, reglas y buenas prácticas que determinan el modo en que todos los activos y recursos, incluyendo la información son gestionados, protegidos y distribuidos dentro de una organización a la hora de implantar un sistema de gestión de seguridad de la Información una organización debe contemplar los siguientes aspectos: (1) formalizar la gestión de la seguridad de la información, (2) analizar y gestionar los riesgos, (3) establecer procesos de gestión de la seguridad siguiendo la metodología PDCA: Plan, selección y definición de medidas y procedimientos, Do, implantación de medidas y procedimientos de mejora, Check**,** comprobación y verificación de las medidas implantadas, Act, actuación para corregir todas las deficiencias detectadas en el sistema, (4) Certificación de la gestión de la seguridad.(p. 64)

En todo este proceso es necesario contemplar un modelo que tenga en cuenta los aspectos tecnológicos, organizativos, el cumplimiento del marco legal y la importancia del factor humano, tal y como se presenta en la siguiente figura:

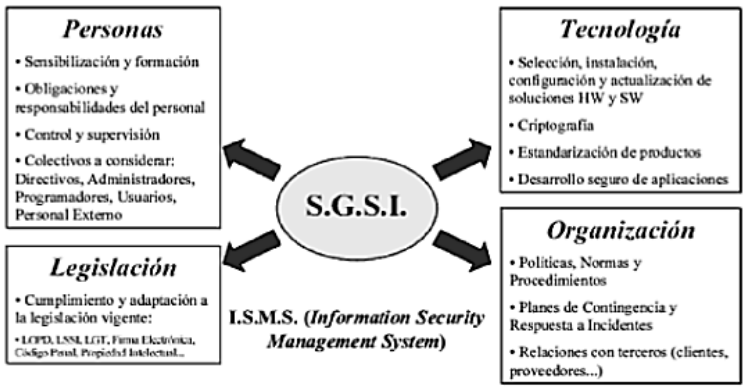


Figura 9. Modelo para la gestión de la seguridad de la información
Tomado de “Enciclopedia de la Seguridad Informática,” RAMA (Segunda ed.), por Gómez, 2014. Madrid, España: Autor.

En este escenario resulta de vital importancia conseguir el soporte adecuado por parte de la dirección de la organización, ya que ésta debe proporcionar la autoridad suficiente para poder definir e implantar las políticas y procedimientos de seguridad, dotando además a la organización de los recursos técnicos y humanos necesarios y reflejando su compromiso en los propios documentos que contienen las principales directrices de seguridad de la organización. De hecho, en algunas organizaciones se ha definido la figura del responsable de gestión de seguridad de la Información, conocido por sus siglas en ingles CISO (Chie Information Security Officer). Podemos distinguir varias etapas o niveles de madurez en la gestión de la seguridad de la Información en una organización: (1) Implantación de medidas básicas de seguridad por sentido común**,** en una primera etapa la organización se preocuparía de la implantación de las medidas básicas de seguridad aplicadas por "sentido común": realización de copias de seguridad, control de acceso a los recursos informáticos, etcétera. Podemos considerar que muchas de las empresas se encuentran todavía hoy en día en esta primera etapa, aplicando unas mínimas medidas de seguridad que pueden resultar insuficientes para garantizar una adecuada gestión de los riesgos, (2) adaptación a los requisitos del marco legal y de las exigencias de los clientes, En esta segunda etapa la organización toma conciencia de la necesidad de cumplir con las exigencias de la legislación vigente o de otras derivadas de sus relaciones y compromisos con terceros (clientes, proveedores u otras instituciones): protección de los datos de carácter personal , delitos informáticos, protección de la propiedad intelectual, (3) gestión de la seguridad de la información, en la tercera etapa la organización ya se preocupa de gestiona planteamiento global e integrado la Seguridad de la Información, la definición de una serie de Políticas de Seguridad, la implantación de planes y procedimientos de seguridad, el análisis y gestión de riesgos, definición de un plan de respuesta a incidentes y de continuidad de negocio, (4) certificación de la gestión de la seguridad de la información**,** Por último, en la cuarta etapa se pretende llevar a cabo una certificación de la gestión de la seguridad de la información, para obtener reconocimiento de las buenas prácticas implantadas por la organización y poder acreditarlo ante terceros (confianza y verificabilidad por terceros): clientes, administraciones públicas y otras instituciones para ello, se

recurre a un proceso de certificación basado en estándares ISO 27001. (Indecopi, 2014).

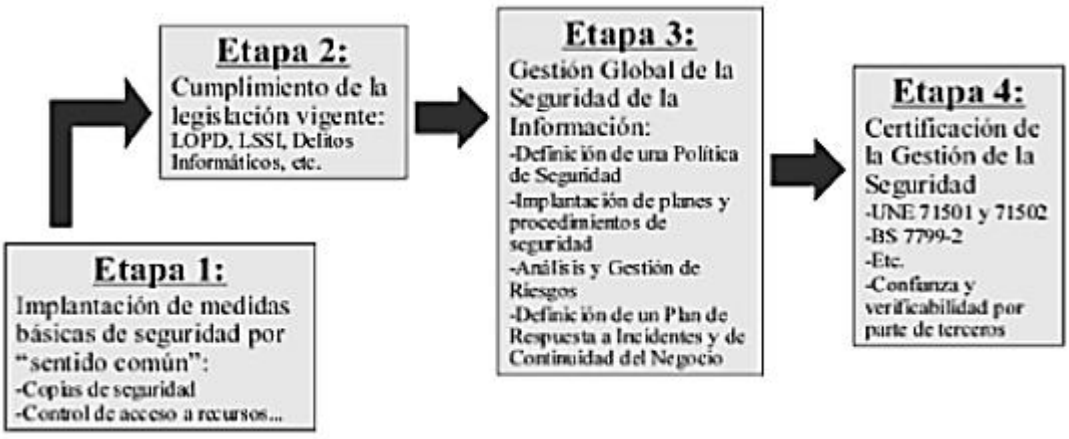


Figura 10. Niveles de madurez del SGSI en la organización
Tomado de "Enciclopedia de la Seguridad Informática," RAMA (Segunda ed.), por Gómez, 2014. Madrid, España: Autor.

Implantación de un sistema de gestión de seguridad de la información

Seguidamente se presenta una guía compuesta por 10 etapas o fases necesarias para la implantación de un SGSI en una organización:

> Gómez (2014), definió 10 etapas: (1) Definición de las políticas de seguridad y del alcance del SGSI**:** definición de las partes o áreas del negocio que van a ser auditadas bajo la norma, especificación del alcance del proyecto identificando los procesos de negocio, los recursos de información, los recursos tecnológicos y organizativos, las personas clave y las relaciones con terceros; establecimiento de las Políticas de Seguridad: la Dirección General, junto con los empleados de los departamentos afectados en la implantación, debe definir y desarrollar una Políticas de seguridad de la Información dentro de la organización, elaboración de un Documento de Seguridad en el que se debe reflejar el compromiso de la Dirección, la definición de la seguridad de la información dentro de su organización, la descripción de los principios fundamentales del sistema de gestión de seguridad de la información, la definición de las

responsabilidades de los usuarios, la referencia al soporte documental y el cumplimiento con los requisitos legales y contractuales, (2) Definición de responsabilidades y asignación de recursos: creación de un comité de seguridad que se encargará de la revisión y actualización de las políticas de seguridad de la Información; este comité revisará el análisis de riesgos. Partiendo de la identificación de los principales activos y recursos a proteger, de sus vulnerabilidades y de las posibles amenazas que les puedan afectar. Asimismo, se debería definir un responsable de la implantación del SGSI, con la misión de apoyar al Comité de Seguridad, dirigir y mantener el SGSI, trabajar con los procesos y departamentos directamente implicados en el SGSI (actuando de interlocutor con los responsables de los activos identificados y de la correcta implantación del sistema en su proceso o área de negocio) y llevar a cabo las auditorías internas que permitan controlar la adecuada implantación del SGSI. (3) Identificación y registro de activos: identificación y descripción de todos los activos contemplados dentro del alcance del SGSI, así como de quiénes son los responsables de gestionar dichos activos, (4) Análisis y gestión de riesgos: identificación de amenazas, vulnerabilidades y probabilidades de impacto en los activos. Elaboración de un documento donde se refleje el resultado de la evaluación de las vulnerabilidades, los niveles de riesgo y la necesidad de aplicar las distintas medidas y requisitos de seguridad, (5) Selección e implantación de controles de seguridad: elaboración de un documento de selección de controles de seguridad. Revisión de la aplicabilidad de los controles seleccionados. Implantación de forma efectiva de los controles seleccionados, (6) Establecer un programa de mejora de la seguridad: definición de un plan de acción con actuaciones concretas para mejorar la seguridad, siguiendo el modelo "PDCA", (7) Completar la documentación del SGSI**:** planificación y diseño del SGSI, incluyendo la definición del alcance, políticas de seguridad de la información, registro de activos de información y valoración de riesgos, documento de selección de

> controles (DSC), procedimientos para la implantación de los controles, procedimientos para la gestión y operación del SGSI, (8) Revisión y auditoría interna del proyecto de implantación del SGSI, (9) Realización de la auditoría de certificación, (10) Ejecutar las recomendaciones de la auditoría. (pp. 69-71)

Dimensiones de la variable dependiente seguridad de la información

Dimensión 1: Técnico

Como lo estableció (Gómez, 2012) “el plano técnico se mide de acuerdo al servicio de selección, instalación, configuración y actualización de soluciones de hardware y software, criptografía, estandarización de productos, desarrollo seguro de aplicaciones” (p. 48). Es decir través de peritaje y reconocimiento físico se establece la memoria fotográfica que da soporte a los informes de estado actual de la organización en cuanto a su infraestructura física evaluando temas como controles de acceso y continuidad del servicio. Uno de los procedimientos más críticos se aborda en el análisis de recursos lógicos, dado que para lograr determinar el estado en cuanto a seguridad de la información de los recursos lógicos es necesario realizar detección de vulnerabilidades, test de penetración, entre otros, en ambientes controlados con el fin de detectar vulnerabilidades tales como el acceso no autorizado.

Dimensión 2: Legal

Gómez (2014), definió: “esta dimensión nos va a permitir regular el mundo informático en la institución de estudio evitando que se convierta en una jungla donde siempre sale ganando el más fuerte” (p.48), fruto del mismo son: (1) el cumplimiento y adaptación de la legislación vigente, (2) propiedad intelectual, (3) firma digital, (4) comercio electrónico, (5) delitos informáticos, (6) código penal entre otras materias. En definitiva lo que se protege en términos informáticos no es simplemente el almacenamiento de obras , su ordenación y recuperación, sino que es todo el procedimiento de creación y resultado final de la misma, en cuanto a su contenido, análisis, almacenamiento, clasificación, selección y ordenación que caracteriza a los sistemas de información en sí. El incumplimiento de la legalidad informática se podría definir como un delito informático, es decir toda

acción (acción u omisión) culpable realizada por un ser humano, que cause un perjuicio a personas sin que necesariamente se beneficie el autor o que, por el contrario, produzca un beneficio ilícito a su autor aunque no perjudique de forma directa o indirecta a la víctima tipificado por la ley, que se realiza en el entorno informático y está sancionado con una pena, como se puede apreciar esta dimensión nos permitirá medir cuan preparado está el SGSI para cualquier atentado informático.

Dimensión 3: Humano

Gómez (2014), nos dijo que: “en este plano la sensibilización y formación de empleados y directivos es importante; así como la definición de sus funciones y obligaciones”, (p. 48). La organización define con claridad cuáles son los distintos niveles de accesos a los servicios y recursos del sistema de informático por parte de los colaboradores y directivos; de la misma manera se deberá informar puntualmente a los colaboradores con acceso al sistema de información de cuáles son sus obligaciones en materia de seguridad; se deberán llevar a cabo acciones de formación de forma periódica para mejorar los conocimientos informáticos y en materia de seguridad de estos empleados . Las personas que se incorporen a la organización tendrán que ser informadas y entrenadas de forma adecuada, sobre todo en las áreas de trabajo con acceso a datos sensibles y aplicaciones importantes para el funcionamiento de la organización., esta dimensión será medida por medio de entrevistas y encuestas aplicadas al personal de las áreas involucradas en procesos seleccionados a incluir en el SGSI y así establecer un marco de referencia que permitirá identificar el estado del arte de la organización frente a la seguridad de la información desde las perspectivas de sus trabajadores además de las competencias de estos en dichos temas.

Dimensión 4: Organizativo

Gómez (2014), definió: “esta dimensión establece la política de seguridad de la información que es el marco que establece los alcances y objetivos del SGSI”; (p.49). Por su parte, los planes de seguridad son documentos de tipo ejecutivo que aplican controles, acciones preventivas y correctivas establecidas a través del tratamiento del riesgo y complementado con buenas prácticas para el

cumplimiento por parte del personal de la organización y terceras partes, una vez finalizados estos documentos, deben contar con el aval de la dirección de la organización y deben establecer el inicio del SGSI, sigue a este proceso la educación en seguridad de la información a todo el personal y el establecimiento de auditorías y mejoramiento continuo, Cada cierto tiempo, como lo establece el estándar ISO/IEC 27001, deben realizarse actualizaciones y mejoras a los planes, adecuándolos según la introducción de nuevos procesos y tecnologías. La construcción de la política de seguridad de la información para la organización es un proceso en conjunto con todas las áreas de la organización involucradas con las tecnologías de la información y cuyos procesos hacen parte del SGSI, esta política establece el lineamiento de la organización frente a la seguridad de la información y es la hoja de ruta que deben cumplir los objetivos del SGSI. Finalmente, se realiza el establecimiento de los planes de seguridad a través de los cuales la organización implementará los controles establecidos para sus procesos; para el establecimiento de los planes de seguridad se hará uso de estándares internacionales, guías y librerías de buenas prácticas en tecnologías de la información y seguridad, certificaciones internacionales de seguridad de la información, normas y/o leyes nacionales aplicables. (Borbón, 2013).

Importancia de la seguridad de la información en el programa de desarrollo agrario rural

Agrorural (2017) a fin de que cumplir con los objetivos estratégicos en los que las TICS están consideradas en Agrorural, es imprescindible que la seguridad sea: mínimamente intrusiva: que no dificulte innecesariamente la actividad diaria ni hipoteque alcanzar los objetivos de productividad propuestos, sea “natural”: que no dé pie a errores gratuitos, que facilite el cumplimiento de las buenas prácticas propuestas.

Es importante la participación de la alta dirección que tomará la decisión de la implantación de un SGSI, que gracias al presente estudio facilitara dicha decisión, el cual pregonara con el ejemplo en la actividad diaria y reaccione con presteza a los cambios e incidencias. Permitirá que la seguridad de la información pueda cuantificar la capacidad de las redes o de los sistemas de información para resistir, con un determinado nivel de confianza, los accidentes o acciones ilícitas o

malintencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos y de los servicios que dichas redes y sistemas ofrecen o hacen accesibles. El objetivo a proteger es la misión de la Organización, teniendo en cuenta las diferentes dimensiones de la seguridad: (1) Técnico, (2) legal, (3) humano y Organizativo.

1.4 Formulación del problema

La constante evolución de las tecnologías de la información ha generado la necesidad de una evaluación periódica para verificar el nivel de riesgo a la que pueda estar expuestos los activos de la información. En el Programa de Desarrollo Productivo Agrario Rural La gestión de riesgos de TI se realiza de manera incipiente, casi nula lo que genera un inadecuado proceso de seguridad de la información, es decir debido a que no hay una política de gestión de riesgos de ti adecuado, se genera una deficiente seguridad de la información.

No existe una adecuada gestión de riesgos por lo se hace necesario evaluar la instalación y configuración de todos los componentes de información, tales como servidores de datos, computadoras clientes, medios de acceso, etc. Existe una ejecución de un plan de difusión y sensibilización por parte del Estado a través del ONGEI del tratamiento de Gestión de riesgos Informáticos a nivel nacional así como la aplicación del sistema de gestión de seguridad de la información, los cuales no están cumpliendo a cabalidad por parte de la institución en estudio, esto aunado a que en el Perú existe una brecha digital entre zonas rurales y urbanas, que se convierte en el obstáculo principal para convertir al país en una Sociedad de la Información que traerá consigo su desarrollo por lo que el riesgo de información es inminente.

Las TIC tienen como fin conectar al mundo de forma rápida y segura, logrando que todos tengan las mismas oportunidades de informarse y, por lo tanto, generar conocimiento de manera segura evitando los fraudes informáticos o mal uso de estas herramientas TIC, sin embargo, en la actualidad, existen varios síntomas visibles que indican que el área de TI de Agrorural no cumple con las expectativas que espera el negocio. Los síntomas presentados son: inadecuada gestión de la infraestructura de TI, excesos de gastos al apagar incendios de TI y no aplicar soluciones definitivas, fallas en el cumplimiento a las regulaciones de

los distintos organismos rectores en tecnología, incumplimiento de los niveles de servicio con los clientes internos y externos, quejas recurrentes por parte de los colaboradores, entre otros.

Sin un plan para identificar la magnitud de amenaza de ejecución del riesgo en la seguridad de la información en Agrorural es imposible un seguimiento y control del riesgo por parte del personal encargado de asegurar la continuidad operativa tecnológica de la institución. En este contexto para el Programa de Desarrollo Productivo Agrario Rural es de vital importancia el manejo de la información de forma adecuada y oportuna para las mejores decisiones, esta debe de estar disponible, integra y confiable por ello es necesario identificar, analizar y tratar los riesgos de TI. Actualmente Agrorural cuenta con más de oficinas desconcentradas las cuales necesitan intercambiar información para realizar sus labores cotidianas como por ejemplo el uso ininterrumpido del internet, el correo electrónico institucional, su seguridad perimetral contra cualquier ataque informático, la conectividad en línea con sus sedes, la accesibilidad de los sistemas en web y que seguridad se proporciona a los mismos.

Entonces llegamos a la conclusión que la continuidad del negocio tecnológico en la institución de estudio se basa en la identificación, análisis y tratamiento de los riesgos de infraestructura tecnológica, para ello se hace necesario la identificación de todos los activos que estén dentro de la gestión tecnológica para su adecuado tratamiento del riesgo y medir su influencia en la seguridad informática, en nuestra investigación nos respaldaremos en la metodología de Margerit, que combina adecuadamente las ISO 27001:2013 Sistema de seguridad de la información y la ISO 31000 gestión de riesgos el cual nos ayudara a tener un ambiente proyectado a un mejor tratamiento de los riesgos en la seguridad de la información.

1.4.1 Problema general

¿En qué medida la gestión de riesgos de TI influye en la seguridad de la información del Programa de Desarrollo Productivo Agrario Rural 2017?

1.4.2 Problemas específicos

Primer problema específico

¿En qué medida la gestión de riesgos de los activos de información de TI influye en la seguridad de la información del Programa de Desarrollo Productivo Agrario Rural 2017?

Segundo problema específico

¿En qué medida la gestión de riesgos de las amenazas de TI influye en la seguridad de la información del Programa de Desarrollo Productivo Agrario Rural 2017?

Tercer problema específico

¿En qué medida el impacto potencial de ejecución de riesgos de TI influye en la seguridad de la información del Programa de Desarrollo Productivo Agrario Rural 2017?

Cuarto problema específico

¿En qué medida la gestión del riesgo potencial de TI influye en la seguridad de la información del Programa de Desarrollo Productivo Agrario Rural 2017?

Quinto problema específico

¿En qué medida la aplicación de salvaguardas a los riesgos de TI influyen en la seguridad de la información del Programa de Desarrollo Productivo Agrario Rural 2017?

1.5 Justificación del estudio

1.5.1 Justificación teórica

El presente trabajo de investigación surge por la necesidad demostrar que, la tecnología soporta los procesos de negocio de información por lo cual es necesario realizar una eficiente administración de riesgos de TI, para conocer si nuestros activos tecnológicos que sobrelleva los procesos de negocio reúne los

requisitos mínimos necesarios para poder seguir prestando el servicio de apoyo tecnológico a la institución. Actualmente muy pocas entidades del estado están implementando la práctica de gestión de riesgos en TI, es por eso que he decidido realizar esta investigación con el propósito de determinar cuál es la importancia de la función de la administración de riesgos en TI y su implicancia en la seguridad de la información promoviendo esta función dentro del Programa de Desarrollo Productivo Agrario Rural del Minagri. Es importante subrayar que un modelo de administración de riesgos asociados a las TI es independiente de que la institución siga o no funcionando de la misma forma, ni son vinculantes sus conclusiones. Queda a cargo de la institución tomar las decisiones pertinentes. Considerando que por su relevancia debería tener carácter ejecutivo

1.5.2 Justificación practica

La identificación y análisis de un riesgo implica la consideración de las causas y las fuentes de riesgo, sus consecuencias positivas y negativas y la probabilidad de que estas consecuencias puedan ocurrir. Se debe identificar los factores que afectan a las consecuencias y a la probabilidad, porque con los resultados o conclusiones que se obtendrán van a favorecer e involucrar a todos los colaboradores del Programa de Desarrollo Productivo Agrario Rural (autoridades, funcionarios, trabajadores) transformando a su gestor de tecnologías de la información en líder en su institución. Él planifica, organiza, dirige, supervisa y controla la gestión de riesgos y la seguridad de la información asegurando la continuidad operativa de la institución mejorando su accionar dentro de la entidad, además nos permitirá obtener un nuevo conocimiento sobre la aplicación de un control de riesgos que garantizara que las herramientas tecnológicas contribuyan a la toma de decisiones y lograr la eficiencia y eficacia de la gestión administrativa, por ende de la gestión de Agrorural, que logrará un impacto positivo en la población.

1.5.3 Justificación metodológica

La investigación se realizará teniéndose en consideración los procedimientos del sistema de investigación científica, dado que se empleará el cuestionario como instrumento de recolección de información, se validará y se determinará su

viabilidad. Ello permitirá a otros investigadores e incluso a los mismos colaboradores de la entidad a poner en práctica el método científico para resolver los problemas que se presenten en la entidad. Con el presente estudio permitirá demostrar que con la aplicación de un programa basado en gestión por resultados se mejora una gestión administrativa, y puede ser utilizado por instituciones similares, es un aporte como fuente de conocimiento y antecedente para la realización de futuras investigaciones en el campo de gestión tecnológica y en la solución de una serie de problemas que afectan directa e indirectamente la gestión pública.

Hipótesis

1.5.4 Hipótesis general

La gestión de riesgos de TI influye en la seguridad de la información del Programa de Desarrollo Productivo Agrario Rural 2017.

1.5.5 Hipótesis especificas

Hipótesis específica 1

La gestión de riesgos de activos de información de TI influye en la seguridad de la información del Programa de Desarrollo Productivo Agrario Rural 2017.

Hipótesis específica 2

La gestión de riesgos de las amenazas de TI influye en la seguridad de la información del Programa de Desarrollo Productivo Agrario Rural 2017.

Hipótesis específica 3

El impacto potencial de ejecución de riesgos de TI influye en la seguridad de la información del Programa de Desarrollo Productivo Agrario Rural 2017.

Hipótesis específica 4

La gestión del riesgo potencial de TI influye en la seguridad de la información del Programa de Desarrollo Productivo Agrario Rural 2017.

Hipótesis específica 5

La aplicación de salvaguardas a los riesgos de TI influye en la seguridad de la información del Programa de Desarrollo Productivo Agrario Rural 2017.

1.6 Objetivos

1.6.1 Objetivo general

Determinar la influencia de la gestión de riesgos de TI en la seguridad de la información del Programa de Desarrollo Productivo Agrario Rural.

1.6.2 Objetivos específicos

Primer objetivo específico

Identificar la influencia de la gestión de riesgos de los activos de información de TI en la seguridad de la información del Programa de Desarrollo Productivo Agrario Rural 2017.

Segundo objetivo específico

Medir la influencia de la gestión de riesgos de las amenazas de TI en la seguridad de la información del Programa de Desarrollo Productivo Agrario Rural 2017.

Tercer objetivo específico

Reconocer la influencia del impacto potencial de ejecución de riesgos de TI en la seguridad de la información del Programa de Desarrollo Productivo Agrario Rural 2017.

Cuarto objetivo específico

Definir la influencia de la gestión de riesgo potencial de los activos de información de TI en la seguridad de la información del Programa de Desarrollo Productivo Agrario Rural 2017.

Quinto objetivo específico

Verificar la influencia de la aplicación de salvaguardas a los riesgos de TI en la seguridad de la información del Programa de Desarrollo Productivo Agrario Rural 2017.

.

II. Marco metodológico

2.1 Variables

En la presente investigación se establecerán como variables de estudio la gestión de riesgos y la seguridad de la información. Ambas variables son de naturaleza cuantitativa de escala ordinal, es decir que se pueden establecer influencias de orden entre las variables, lo que va a permitir establecer influencias de tipo mayor, menor, igual o niveles entre ellas.

Definición conceptual de la variable independiente gestión de riesgos

Magerit (2012) nos definió que: “la gestión del riesgo se divide en dos tareas: (1) análisis del riesgo y (2) tratamiento de los riesgos; los cuales no son un fin en sí mismas, sino que se encajan en la actividad continua de gestión de la seguridad” (p. 10), el análisis de riesgos permite determinar cómo es, cuánto vale y cómo de protegido se encuentra el sistema. En coordinación con los objetivos, estrategia y política de la organización, las actividades de tratamiento de los riesgos permiten elaborar un plan de seguridad que, implantado y operado, satisfaga los objetivos propuestos con el nivel de riesgo que acepta la dirección, por lo que se deduce que el análisis de riesgos proporciona un modelo del sistema en términos de activos, amenazas y salvaguardas que se acometen en materia de seguridad para satisfacer las necesidades detectadas por el análisis.

Definición operacional de la variable independiente gestión de riesgos

La variable independiente gestión del riesgo, contempla cinco planos de actuación o dimensiones: (a) Activos de información, que son los elementos del sistema de información (o estrechamente relacionados con este) que soportan la misión de la Organización, se midió con cinco ítems; (b) Amenazas, que son cosas que les pueden pasar a los activos causando un perjuicio a la Organización, se midió con cuatro ítems; (c) Impacto potencial: lo que podría pasar, se midió con cuatro ítems; (d) Riesgo potencial: lo que probablemente pase, se midió con dos ítems (e) Salvaguardas (o contra medidas), que son medidas de protección desplegadas para que aquellas amenazas no causen tanto daño, se midió con 6 ítems. Esta variable fue medida con un instrumento constituido por 21 ítems con respuesta tipo Likert y los rangos establecidos fueron baja de 21-49, moderada de 50-77, alta de 78-105, que nos permitirá evaluar su influencia en la seguridad de la

información en el Programa de Desarrollo Productivo Agrario Rural 2017.

Definición conceptual de la variable dependiente seguridad de la información

Gómez (2014) estableció que: “la seguridad de la información es cualquier medida que impida la ejecución de operaciones no autorizadas sobre un sistema o red informática” (p. 34), cuyos efectos puedan conllevar daños sobre la información, comprometer su confidencialidad, autenticidad o integridad, disminuir el rendimiento de los equipos o bloquear el acceso de usuarios autorizados al sistema, Asimismo, es necesario considerar otros aspectos o cuestiones relacionados cuando se habla de Seguridad Informática: (1) cumplimiento de las regulaciones legales aplicables a cada sector o tipo de organización, dependiendo del marco legal de cada país, (2) control en el acceso a los servicios ofrecidos y la información guardada por un sistema informático, (3) control en el acceso y utilización de ficheros protegidos por la ley: contenidos digitales con derechos de autor, ficheros con datos de carácter personal, etcétera, (4) Identificación de los autores de la información o de los mensajes

Definición operacional de la variable dependiente seguridad de la información

La variable seguridad de la información, contempla cuatro planos de actuación o dimensiones: (a) Técnico, tanto a nivel físico como a nivel lógico, se midió con cinco ítems; (b) Legal, algunos países obligan por Ley a que en determinados sectores se implanten una serie de medidas de seguridad (sector de servicios financieros y administrativos, protección de datos personales, delitos informáticos, código penal, propiedad intelectual, gobierno electrónico, etcétera), se midió con 3 ítems; (c) Humano, sensibilización y formación de empleados y directivos, definición de funciones y obligaciones del personal, se midió con 3 ítems; (d) Organizativo, definición e implantación de políticas de seguridad, planes, normas, procedimientos y buenas prácticas de actuación, se midió con 5 ítems. Esta variable fue medida con un instrumento constituido por 16 ítems con respuesta tipo Likert y los rangos establecidos fueron bajo de 21-49, moderado de

49-77, alto de 77-105.permitirá medir como está siendo influida por la gestión de riesgos de ti, el grado de seguridad de información existente en el Programa de Desarrollo Productivo Agrario Rural 2017

2.2 Operacionalización de variables

Tabla 1

Matriz de operacionalización de la variable gestión de riesgos

Dimensiones	Indicadores	Ítems	Escala de medición y valores	Niveles y rangos
Activos de información	Activos esenciales	1, 2,3,4		
Amenazas	Servicios internos Equipamiento informático Identificación amenazas	4,5 6,7,8,9	1=completamente en desacuerdo 2=En desacuerdo 3=Ni de acuerdo, ni desacuerdo 4=De acuerdo 5= Completamente de acuerdo	Baja 21 - 49 Moderada 50 - 77 Alta 78 - 105
Impacto potencial	valoración Impacto acumulado Impacto repercutido	10,11 12 13		
Riesgo potencial	Riesgo acumulado Riesgo repercutido	14 15		
Salvaguardas	Selección salvaguardas Efectos de las salvaguardas	16,17,18, 19,20,21		

Tabla 2

Matriz de operacionalización de la variable seguridad de la información

Dimensiones	Indicadores	Ítems	Escala de medición y valores	Niveles y rangos
Técnico	Instalación Configuración Criptografía Estandarización Desarrollo de Aplicación con enfoque de seguridad	1 2 3 4 5	1=completamente en desacuerdo 2=En desacuerdo 3=Ni de acuerdo, ni desacuerdo 4=De acuerdo 5= Completamente de acuerdo	Deficiente 16 - 37 Regular 38 -59 Eficiente 60 - 80
Legal	Cumplimiento y adaptación de la legislación vigente LSSI Firma Electrónica Propiedad Intelectual	6 7 8		
Humano	Sensibilización y formación. Funciones y obligaciones Control y supervisión de los trabajadores	9 10 11		
Organizativo	Políticas Normas Directivas Procedimientos Planes de Contingencia y Respuesta a Incidentes Relaciones con terceros (clientes, proveedores)	12 13 14 15 16		

2.3 Metodología

El trabajo se desarrolló bajo un enfoque cuantitativo pues baso en la recolección de datos para probar hipótesis, en función de una medida numérica y el respectivo análisis estadístico, para establecer patrones de comportamiento y probar teorías al describir variables (investigación descriptiva). Permitirá determinar las interacciones causa-efecto entre las variables (investigación cuasi experimental) y realizar el análisis de causa-efecto. (Fernández y Baptista, 2010).

Por lo expuesto el método usado fue el hipotético deductivo, que es la base de toda investigación científica. Se realizó la observación del fenómeno a estudiar, en base a las cuales se plantearon los problemas e hipótesis respectivas y luego del análisis correspondiente se verifico y comprobó la verdad de los enunciados deducidos. Este método combina la reflexión racional (la formación de hipótesis y la deducción) con la observación de la realidad (la observación y la verificación) (Lorenzano, 2010).

2.4 Tipo de estudio

La investigación fue básica de nivel descriptivo y de análisis causa-efecto según la clasificación de (Hernández, Fernández y Baptista, 2010).

Básica, porque busca nuevos conocimientos sin un fin practico inmediato; está dedicada a ampliar los conocimientos relacionados a las variables gestión de riesgos y seguridad de la información.

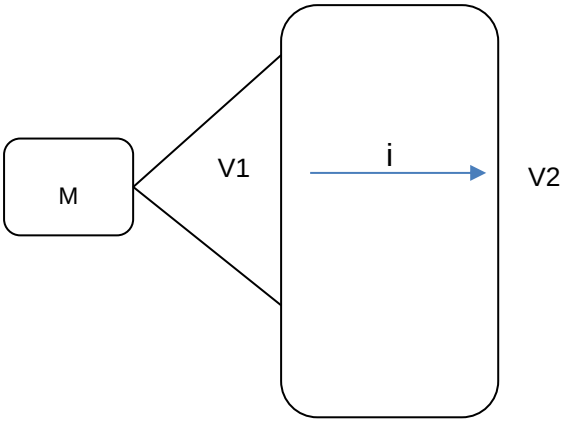
Descriptiva, pues se describió a cada una de las variables de estudio tal y cual se presentaron al momento de la investigación.

Causa-efecto porque midió el grado de influencia que existía entre la variable gestión de riesgos y la seguridad de la información en el Programa de Desarrollo Productivo Agrario rural.

2.5 Diseño

La investigación obedece a un diseño no experimental de corte transversal, pues no se desarrolló ningún tratamiento experimental y la recolección de datos se

realizó en un solo momento (Hernández, Fernández y Baptista, 2010) y obedece al siguiente esquema:



Dónde:

M → Muestra

V1 → Variable 1

V2 → Variable 2

I → Representa la influencia de V1 en V2

2.6 Población, muestra y muestreo

2.6.1 Población

La población estuvo conformada por 174 colaboradores de la sede central del Programa de Desarrollo Productivo Agrario rural.

Se consideran como criterios de inclusión, el estar laborando en la institución en alguna área específica con una antigüedad laboral de 1.5 años, por considerarlo un periodo en el que le ha permitido conocer las características del Programa de Desarrollo Productivo Agrario Rural donde se desarrolla la investigación.

2.6.2 Muestra

Bernal (2010), define la muestra como: “la parte de la población que se selecciona, de la cual realmente se obtiene información para el desarrollo del estudio y sobre la cual se efectuará la medición y observación de las variables

objeto de estudio". (p. 161)

La presente investigación obtuvo el tamaño de la muestra luego de aplicar la siguiente formula estadística de población conocida:

$$n = \frac{N * Z_{\alpha}^{2} p * q}{d^{2} * (N-1) + Z_{\alpha}^{2} * p * q}$$

Dónde:

N = Total de la población

$Z_a^2 = (1.96)^2$ (si la seguridad es del 95%)

p = Probabilidad de ocurrencia

q = (1-p) (Probabilidad de no ocurrencia)

d = precisión (en este caso deseamos un 5%).

Se consideraron los siguientes supuestos:

Tamaño poblacional (N) = 174

Error máximo admisible (e) = 5%.

Nivel de confianza = 95% (equivale a Z=1.96)

p=0.5

q=0.5

$$n = \frac{(174)(3.8416)(0.5)(0.5)}{(0.0025)(120-1) + (3.8416)(0.5)(0.5)} = 119.8686$$

Reemplazando y redondeando se obtiene n = 120

2.6.3 Muestreo

Para la presente investigación se empleó el muestreo aleatorio estratificado, con esta técnica de muestreo se logró que todos los elementos que forman parte del universo de la población tengan la misma posibilidad de ser parte del estudio.

Al respecto, (Hernández, Fernández y Baptista, 2010), expresaron que la muestra probabilística comprende al: "subgrupo de la población en el que todo los elementos de esta tienen la misma posibilidad de ser elegidos".

La presente investigación utilizo el numérico de los colaboradores del Programa de Desarrollo Productivo Agrario Rural sede central Lima, y a partir de la generación de números aleatorios del software SPSS Statical Pack age for the Social Science) fueron seleccionados los casos que formaran parte del tamaño de la muestra calculado previamente.

Tabla 3

Número de colaboradores que conforman la muestra de estudio, según oficinas y direcciones

Total	**Colaboradores**
Direccion Ejecutiva	07
Oficina de Planificación y presupuesto	26
Oficina de Asesoria Legal	13
Oficina de Administracion	60
Oficina de Control Interno	08
Direccion de Recursos Naturales	23
Direccion de Desarrollo Agrario	16
Direccion de Infraestructura Agraria y Riego	21
Total	174

2.7 Técnicas e instrumentos de recolección de datos

2.7.1 Técnica

La técnica utilizada en la presente investigación es la encuesta, que es una técnica que “se utiliza para la indagación, exploración y recolección de datos, mediante preguntas formuladas directa o indirectamente a los sujetos que constituyen una unidad de análisis”. (Carrasco, 2013, p.318).

Considerando este aporte se recogió información con la técnica de la encuesta aplicando un cuestionario a los 120 trabajadores del Programa de Desarrollo Productivo agrario rural sede central Lima, 2017.

2.7.2 Instrumentos

Según la técnica de la investigación realizada, el instrumento utilizado para la recolección de información fue el cuestionario. Al respecto Carrasco (2013), indica que “los cuestionarios consisten en presentar a los encuestados unas hojas conteniendo una serie ordenada y coherente de preguntas formuladas, con claridad, precisión y objetividad, para que sean resueltas de igual modo” (p.318).

Ficha técnica del instrumento para medir la gestión de riesgos en el Programa de Desarrollo Productivo Agrario Rural 2017.

Nombre del instrumento	Cuestionario para medir el nivel de la gestión de riesgos de TI en Agrorural 2017.
Autor y Año	Esteban Crespo Martínez (2017).
Adaptado si fuera el caso	Adaptado de Crespo Martínez (2017).
Universo de estudio	174 colaboradores
Nivel de confianza	95.0%
Margen de error	5.0%
Tamaño muestral	120 colaboradores
Tipo de técnica	Encuesta
Tipo de instrumento	Cuestionario
Fecha trabajo de campo	Nov. 2017
Escala de medición	Escala Likert (politómica)
Tiempo utilizado	30 minutos

Ficha técnica del instrumento para medir la seguridad de la información en el Programa de Desarrollo Productivo Agrario Rural 2017.

Nombre del instrumento	Cuestionario para medir el nivel de seguridad de la información de Agrorural 2017.
Autor y Año	Esteban Crespo Martínez (2017).
Adaptado si fuera el caso	Adaptado de Crespo Martínez (2017).
Universo de estudio	174 colaboradores

Nivel de confianza	95.0%
Margen de error	5.0%
Tamaño muestral	120 colaboradores
Tipo de técnica	Encuesta
Tipo de instrumento	Cuestionario
Fecha trabajo de campo	Nov. 2017
Escala de medición	Escala Likert (politómica)
Tiempo utilizado	30 minutos

Validez

Por lo que en términos generales, se refiere al grado en que un instrumento realmente mide la variable que pretende medir (Hernández, Fernández y Baptista, 2010).

Para determinar la validez de los instrumentos, se sometieron a consideraciones de juicio de expertos. Según Hernández, Fernández y Baptista (2010), el juicio de expertos (anexo 04) para contrastar la validez de los ítems consiste en preguntar a personas expertas en el dominio que miden los ítems, sobre su grado de adecuación a un criterio determinado y previamente establecido.

Tabla 4

Juicio de expertos

Especialistas	Opinión de aplicabilidad	
	Gestión de Riesgos	Seguridad de la Información
Dr. Padilla Caballero, Jesús Emilio Agustín.	Aplicable	Aplicable
Dr. Flores Sotelo, William Sebastian.	Aplicable	Aplicable
Dr. Guevara Fernández, Ricardo.	Aplicable	Aplicable

Fiabilidad

Los instrumentos de recolección de datos que se emplearon en la investigación tiene ítems con opciones en escala Likert, por lo cual se ha utilizado el coeficiente

alfa de Cronbach para determinar la consistencia interna, analizando la correlación media de cada ítem con todas las demás que integran dicho instrumento.

Para determinar el coeficiente de confiabilidad, se aplicó la prueba piloto, después de analizo mediante el alfa de Cronbach con la ayuda del software estadístico SPSS versión 24.

La escala de valores que determina la confiabilidad está dada por los siguientes valores (Escobedo, Mendoza, y Cuervo 2009)

Alrededor de 0.9, es un nivel elevado de confiabilidad.

La confiabilidad de 0.8 o superior puede ser considerada como confiable

Alrededor de 0.7, se considera baja

Inferior a 0.6, indica una confiabilidad inaceptablemente baja.

Tabla 5

Confiabilidad de los instrumentos - Alfa de Cronbach

Instrumento	Alfa de Cronbach	Nº Ítems
Gestión de riesgos	0.812	21
Seguridad de la información	0.804	16

De acuerdo a los resultados y teniendo en cuenta el índice de fiabilidad obtenido por el alfa de Cronbach igual a 0.800 y 0.824, se puede asumir que los instrumentos son confiables y procede su aplicación.

2.8 Métodos de análisis de datos

Una vez recolectados los datos de la investigación, se procedió al análisis estadístico respectivo. Los datos fueron tabulados y se presentan las tablas y figuras de distribución de frecuencias. Los datos fueron tabulados en el software estadístico SPSS V 22.

Debido a que las variables son cuantitativas, se empleó, para la contratación de las hipótesis la prueba no paramétrica de regresión logarítmica ordinal, que es una medida de causa-efecto para variables que requiere mínimamente de un nivel de medición ordinal, de tal modo que los individuos u objetos de la muestra puedan ordenarse por rangos.

El análisis de los datos se realizó con el software estadístico SPSS versión 24, se tabularon los datos, se determinaron los rangos para cada variable, así mismo las frecuencias por dimensiones.

III. Resultados

3.1 Resultados descriptivos.

Tabla 6

Niveles de la gestión de riesgos de TI del Programa de Desarrollo Productivo Agrario Rural 2017

Gestión de riesgos

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	MALA	76	63.3	63.3	63.3
	REGULAR	32	26.7	26.7	90.0
	BUENA	12	10.0	10.0	100.0
	Total	120	100.0	100.0	

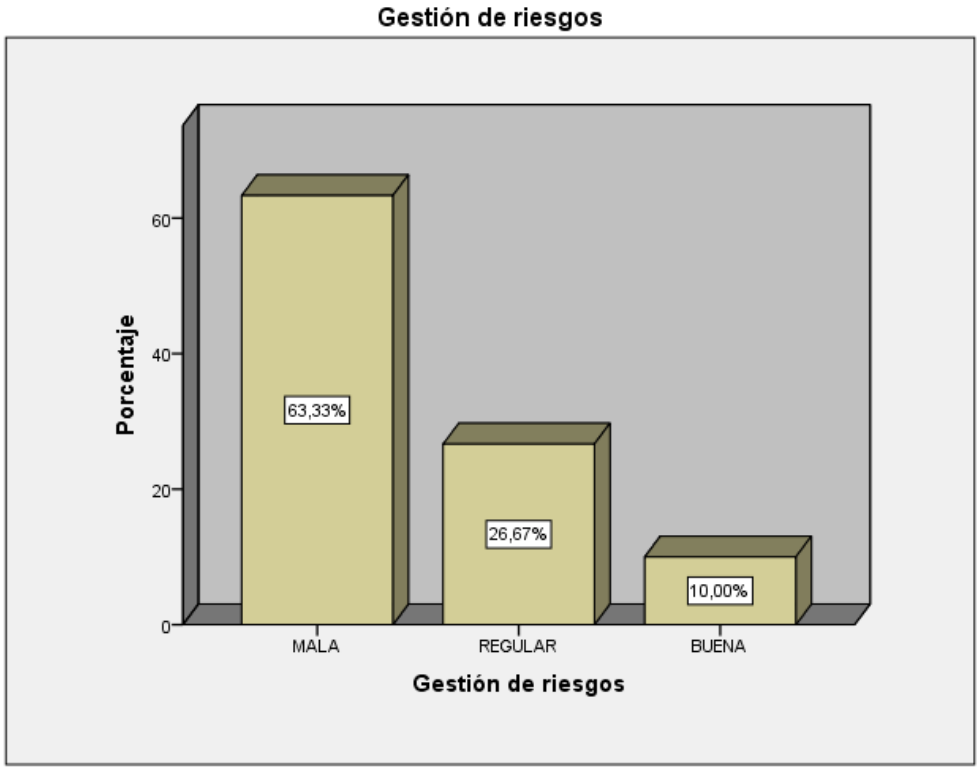


Figura 11. Niveles de la gestión de riesgos en AGRORURAL

De la figura y tabla se aprecian los resultados generales de la gestión de riesgos de TI en el Programa de Desarrollo Productivo Agrario Rural, donde el 63,33% perciben que el nivel es malo en cuanto a la gestión de riesgos, mientras que el 26,67% percibe que el nivel es regular y el 10.00% percibe que el nivel de la gestión de riesgos en el Programa de Desarrollo Productivo Agrario Rural 2017 es bueno. De los resultados en conjunto se tiene que el nivel de la gestión de riesgos de TI en el Programa de Desarrollo Productivo Agrario Rural es mala.

Tabla 7

Niveles de la seguridad de la información en Agrorural 2017.

Seguridad de la información

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	DEFICIENTE	60	50,0	50,0	50,0
	REGULAR	41	34,2	34,2	84,2
	EFICIENTE	19	15,8	15,8	100,0
	Total	120	100,0	100,0	

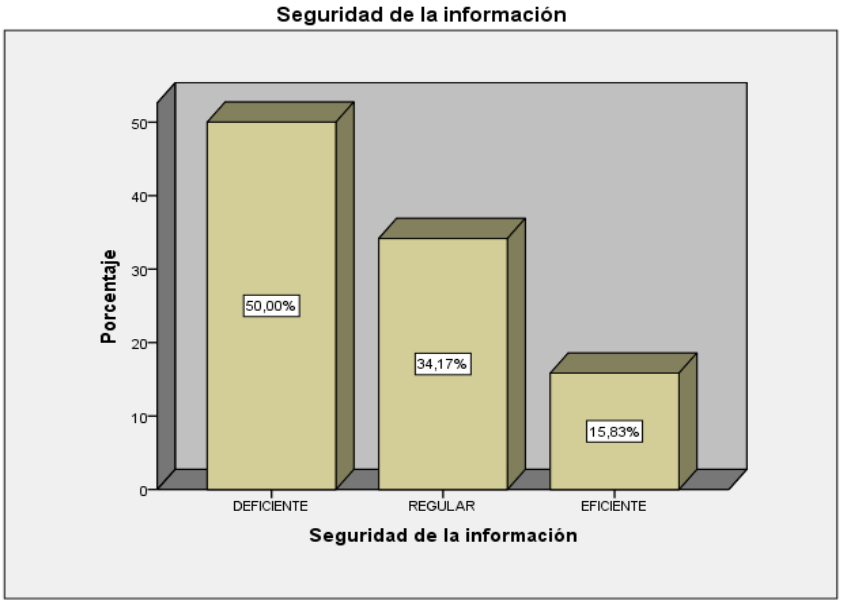


Figura 12 Niveles de la seguridad de la información en Agrorural

De la figura y tabla se aprecian los resultados generales de la seguridad de la información en el Programa de Desarrollo Productivo Agrario Rural, donde el 50,00% perciben que el nivel es deficiente en cuanto a la gestión de seguridad de la información, mientras que el 34,17% percibe que el nivel es regular y el 15,83%

percibe que el nivel es eficiente, en el Programa de Desarrollo Productivo Agrario Rural 2017. De los resultados en conjunto se tiene que el nivel de la seguridad de la información en el Programa de Desarrollo Productivo Agrario Rural 2017 es deficiente.

Resultados previos al análisis de datos

En cuanto a los resultados obtenidos a partir del cuestionario con escala ordinal se asumirá prueba no paramétrica que muestra la dependencia entra la variable independiente frente a la variable dependiente, posteriores a la prueba de hipótesis se basaran a la prueba de regresión logística, ya que los datos para el modelamiento son de carácter cuantitativo ordinal, orientado al modelo de regresión logística ordinal, para el efecto asumiremos el reporte SPSS.

Tabla 8

Ajuste de los datos para el modelo de la gestión de riesgos de TI en la seguridad de la información del Programa de Desarrollo Productivo Agrario Rural 2017.

Información de ajuste de los modelos

Modelo	Logaritmo de la verosimilitud -2	Chi-cuadrado	gl	Sig.
Sólo intersección	44,994			
Final	31,254	22,740	4	.035

Función de enlace: Logit.

En cuanto al reporte del programa a partir de los datos, se tiene los siguientes resultados donde los datos obtenidos estarían explicando la dependencia de la variable de seguridad de la información de la variable gestión de riesgos en el Programa de Desarrollo Productivo Agrario Rural, así mismo se tiene al valor Chi cuadrado es de 22,7 y p_valor (valor de la significancia) es igual a 0.035 frente a la significación estadística α igual a 0.05 (p_valor < α), significa rechazo de la hipótesis nula, los datos de la variable no son independientes, implica la dependencia de una variable sobre la otra.

Tabla 9

Determinación de las variables para el modelo de regresión logística ordinal.

Bondad de ajuste

	Chi-cuadrado	gl	Sig.
Pearson	6,821	8	.716
Desvianza	5,124	8	.704

Función de enlace: Logit.

Así mismo se muestran los resultados de la bondad de ajuste de la variable en el cual no se rechaza la hipótesis nula; por lo que con los datos de la variable es posible mostrar la dependencia gracias a las variables y el modelo presentado estaría dado por el valor estadística de p_valor 0.716 frente al α igual a 0.05. Por tanto, el modelo y los resultados están explicando la dependencia de una variable sobre la otra.

Tabla 10

Estimación de parámetros de la gestión de riesgos en la seguridad de la información del Programa de Desarrollo Productivo Agrario Rural 2017.

Estimaciones de parámetro

							Intervalo de confianza al 95%	
		Estimación	Error estándar	Wald	gl	Sig.	Límite inferior	Límite superior
Umbral	[VAR2_3N = 1]	2,032	1,370	2,200	1	,138	-,653	4,717
	[VAR2_3N = 2]	4,062	1,395	8,481	1	,004	1,328	6,796
	[VAR2_3N = 3]	,687	,544	1,591	1	,000	,380	1,753
Ubicación	[VID1_3N=1]	2,366	1,166	4,118	1	,042	,081	4,652
	[VID1_3N=2]	2,599	1,140	,200	1	,003	,365	4,832
	[VID1_3N=3]	0[a]	.	.	0	.	.	.
	[VID2_3N=1]	,447	,979	,208	1	,648	-1,472	2,367
	[VID2_3N=2]	,322	,928	,420	1	,029	-1,497	2,141
	[VID2_3N=3]	0[a]	.	.	0	.	.	.
	[VID3_3N=1]	-1,009	,833	1,468	1	,226	-2,641	,623
	[VID3_3N=2]	-1,303	,783	,570	1	,006	-2,837	,232
	[VID3_3N=3]	0[a]	.	.	0	.	.	.
	[VID4_3N=1]	-,079	,681	,013	1	,908	-1,414	1,257
	[VID4_3N=2]	,165	,648	,165	1	,009	-1,105	1,435
	[VID4_3N=3]	0[a]	.	.	0	.	.	.
	[VID5_3N=1]	,939	1,043	,510	1	,038	-1,106	2,983
	[VID5_3N=2]	,358	,960	,139	1	,709	-1,524	2,240
	[VID5_3N=3]	0[a]	.	.	0	.	.	.

Función de enlace: Logit.
a. Este parámetro está establecido en cero porque es redundante.

Los resultados en conjunto que se tiene en la tabla muestran los coeficientes de la expresión de la regresión de la gestión de riesgos el nivel bajo (1) frente a la

seguridad de la información en el Programa de Desarrollo Productivo Agrario Rural. Al respecto la variable gestión de riesgos tiene al valor de Wald de 0.200,0.420,0.570,0.165 y 0510; lo que quiere decir que el Programa de Desarrollo Productivo Agrario rural cuenta con una baja gestión de riesgos, por lo que existe la probabilidad de que el grado de seguridad de la información sea deficiente, sin embargo una buena gestión del riesgo tiene la probalidad de que la seguridad de la información sea eficiente, siendo este significativo ya que el p_valor es < al nivel de significancia estadística ($p<0.05$).

Prueba de hipótesis

Ho: La gestión de riesgos de TI no influye en la seguridad de la información en el Programa de Desarrollo Productivo Agrario Rural 2017.

H1: La gestión de riesgos de TI influye en la seguridad de la información en el Programa de Desarrollo Productivo Agrario Rural 2017.

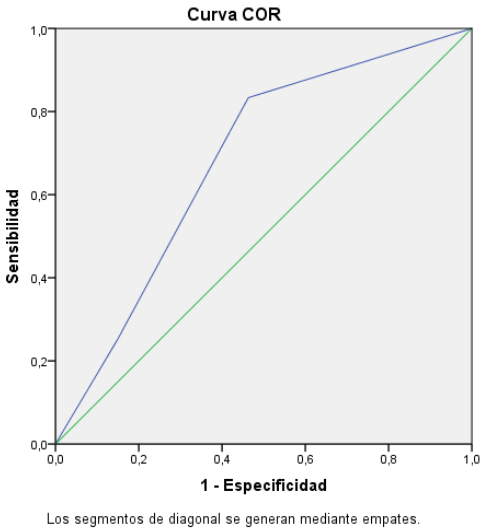
Tabla 11

Prueba de hipótesis general.

Pseudo R cuadrado	
Cox y Snell	.380
Nagelkerke	.440
McFadden	.109

Función de enlace: Logit.

En cuanto de la prueba del pseudo R cuadrado, lo que estarían presentando es la dependencia porcentual de la gestión de riesgos en la seguridad de la información en Agrorural, el cual tiene el coeficiente de Nagalkerke, implicando que la variabilidad de la seguridad de la información depende del 44% de la gestión de riesgos en la seguridad de la información en el Programa de Desarrollo Productivo Agrario Rural.



Área 0.681%

Figura 13. Representación del área COR, como incidencia de la gestión de riesgos en la seguridad de la información.

En cuanto al resultado de la curva COR, se tiene el área que representa la capacidad de clasificación de un 68.1% representando un nivel alto de implicancia de la gestión de riesgos en la seguridad de la información del Programa de Desarrollo Productivo Agrario Rural 2017.

Resultado específico 1

Tabla 12

Estimación de parámetros de la gestión de riesgos de los activos de información en la seguridad de la información del Programa de Desarrollo Productivo Agrario Rural 2017.

Estimaciones de parámetro

							Intervalo de confianza al 95%	
		Estimación	Error estándar	Wald	gl	Sig.	Límite inferior	Límite superior
Umbral	[VAR2_3N = 1]	1,818	1,089	2,789	1	,095	-,316	3,952
	[VAR2_3N = 2]	3,769	1,115	11,425	1	,001	1,583	5,954
	[VAR2_3N = 3]	1,539	,574	7,197	1	,107	,415	2,664
Ubicación	[VID1_3N=1]	2,073	1,124	3,403	1	,065	-,130	4,276
	[VID1_3N=2]	2,415	1,116	,679	1	,031	,227	4,603
	[VID1_3N=3]	0[a]	.	.	0	.	.	.

Función de enlace: Logit.

a. Este parámetro está establecido en cero porque es redundante.

Los resultados en conjunto que se tiene en la tabla muestran los coeficientes de la expresión de la regresión de la gestión de riesgos de los activos de información, el nivel bajo (1) frente a la seguridad de la información. Al respecto el valor de Wald es de 0.679; lo que quiere decir que el Programa de Desarrollo Productivo Agrario Rural cuenta con un bajo nivel de gestión de riesgos de activos de información por lo que la probabilidad de que el nivel de la seguridad de la información sea deficiente, sin embargo una buena gestión del riesgo de los activos de información tiene la probalidad de que la seguridad de la información sea eficiente, siendo este significativo ya que el p_valor es (0.031) < al nivel de significancia estadística (p<0.05).

Prueba de hipótesis especifica 1

Ho: La gestión de riesgos de activos de información de TI no influye en la seguridad de la información del Programa de Desarrollo Productivo Agrario Rural 2017.

H1: La gestión de riesgos de activos de información de TI influye en la seguridad de la información del Programa de Desarrollo Productivo Agrario Rural 2017.

Tabla 13

Prueba de hipótesis especifica 1.

Pseudo R cuadrado	
Cox y Snell	,160
Nagelkerke	,360
McFadden	,250

Función de enlace: Logit.

En cuanto de la prueba del pseudo R cuadrado, lo que estarían presentando es la dependencia porcentual de la gestión de riesgos de los activos de información en la seguridad de la información, el cual tiene el coeficiente de Nagalkerke de 0.360, implicando que la variabilidad de la seguridad de la información depende del 36% de la gestión de riesgos de los activos de información del Programa de Desarrollo Productivo Agrario Rural 2017.

Resultado específico 2

Tabla 14

Estimación de parámetros de gestión de riesgos de las amenazas de TI en la seguridad de la información del Programa de Desarrollo Productivo Agrario Rural 2017.

Estimaciones de parámetro

							Intervalo de confianza al 95%	
		Estimación	Error estándar	Wald	gl	Sig.	Límite inferior	Límite superior
Umbral	[VAR2_3N = 1]	,360	,573	,394	1	,530	-,764	1,484
	[VAR2_3N = 2]	2,243	,616	13,256	1	,000	1,036	3,450
	[VAR2_3N = 3]	1,265	,816	15,256	1	,000	1,536	1,050
Ubicación	[VID2_3N=1]	,298	,613	,237	1	,627	-,904	1,500
	[VID2_3N=2]	,388	,664	,341	1	,009	-,914	1,690
	[VID3_3N=3]	0[a]	.	.	0	.	.	.

Función de enlace: Logit.

a. Este parámetro está establecido en cero porque es redundante.

Los resultados en conjunto que se tiene en la tabla se muestran los coeficientes de la expresión de la regresión de la gestión de riesgos de las amenazas de TI el nivel bajo (1) frente a la seguridad de la información. Al respecto la variable gestión de riesgos tiene al valor de Wald de 0.341; lo que quiere decir que el Programa de Desarrollo Productivo Agrario rural cuenta con un bajo nivel de gestión de riesgos de las amenazas de TI, por lo que la probabilidad de que el nivel de la seguridad de la información sea deficiente, sin embargo una buena gestión del riesgo de las amenazas de TI tiene la probalidad de que la seguridad de la información sea eficiente, siendo este significativo ya que el p_valor es (0.009) < al nivel de significancia estadística (p<0.05).

Prueba de hipótesis especifica 2

Ho: La gestión de riesgos de las amenazas de TI no influye en la seguridad de la información del Programa de Desarrollo Productivo Agrario Rural 2017.

H1: La gestión de riesgos de las amenazas TI influye en la seguridad de la información del Programa de Desarrollo Productivo Agrario Rural 2017.

Tabla 15

Prueba de hipótesis especifica 2.

Pseudo R cuadrado	
Cox y Snell	,300
Nagelkerke	,300
McFadden	,200

Función de enlace: Logit.

En cuanto de la prueba del pseudo R cuadrado, lo que estarían presentando es la dependencia porcentual de la gestión de riesgos de las amenaza de TI en la seguridad de la información, el cual tiene el coeficiente de Nagalkerke de 0.300, implicando que la variabilidad de la seguridad de la información depende del 30% de la gestión de riesgos de las amenazas de TI en la seguridad de la información del Programa de Desarrollo Productivo Agrario Rural 2017.

Resultado específico 3

Tabla 16

Estimación de parámetro del impacto potencial de ejecución riesgos en la seguridad de la información en el Programa de Desarrollo Productivo Agrario Rural 2017

Estimaciones de parámetro

							Intervalo de confianza al 95%	
		Estimación	Error estándar	Wald	gl	Sig.	Límite inferior	Límite superior
Umbral	[VAR2_3N = 1]	-,865	,556	2,421	1	,020	-1,955	,225
	[VAR2_3N = 2]	1,335	,425	5,431	1	,019	,223	2,448
	[VAR2_3N = 3]	1,585	,568	,534	1	,014	,223	2,448
Ubicación	[VID3_3N=1]	-,507	,581	,644	1	,008	-1,660	,645
	[VID3_3N=2]	-,876	,646	,410	1	,016	-2,142	,389
	[VID3_3N=3]	0[a]	.	.	0	.	.	.

Función de enlace: Logit.

a. Este parámetro está establecido en cero porque es redundante.

Los resultados en conjunto que se tiene en la tabla se muestran los coeficientes de la expresión de la regresión del impacto potencial de la ejecución de riesgos el

nivel bajo (1), frente a la seguridad de la información. Al respecto se tiene al valor de Wald de 0.644; lo que quiere decir que el Programa de Desarrollo Productivo Agrario Rural cuenta con un bajo nivel de gestión de impacto potencial de ejecución de riesgos de TI, por lo que la probabilidad de que el nivel de la seguridad de la información sea deficiente, sin embargo una buena gestión de impacto potencial de ejecución de riesgos de TI, tiene la probalidad de que la seguridad de la información sea eficiente, siendo este significativo ya que el p_valor es(0.008) < al nivel de significancia estadística (p<0.05).

Prueba de hipótesis especifica 3

Ho: El impacto potencial de ejecución de riesgos de TI no influye en la seguridad de la información del Programa de Desarrollo Productivo Agrario Rural 2017.

H1: El impacto potencial de ejecución de riesgos de TI influye en la seguridad de la información del Programa de Desarrollo Productivo Agrario Rural 2017.

Tabla 17

Prueba de hipótesis especifica 3.

Pseudo R cuadrado	
Cox y Snell	,150
Nagelkerke	,370
McFadden	,180

Función de enlace: Logit.

En cuanto de la prueba del pseudo R cuadrado, lo que estarían presentando es la dependencia porcentual de la gestión de impacto potencial de la ejecución de riesgos de TI en la seguridad de la información, el cual tiene el coeficiente de Nagalkerke de 0.370, implicando que la variabilidad de la seguridad de la información depende del 37% de la gestión de impacto potencial de riesgos de TI en la seguridad de la información del Programa de Desarrollo Productivo Agrario Rural 2017.

Resultado específico 4

Tabla 18

Estimación de parámetro de riesgos potenciales en la seguridad de la información del Programa de Desarrollo Productivo Agrario Rural 2017.

Estimaciones de parámetro

							Intervalo de confianza al 95%	
		Estimación	Error estándar	Wald	gl	Sig.	Límite inferior	Límite superior
Umbral	[VAR2_3N = 1]	-,478	,542	,776	1	,378	-1,540	,585
	[VAR2_3N = 2]	1,217	,555	4,813	1	,028	,130	2,303
	[VAR2_3N = 3]	1,647	,255	3,813	1	,008	,130	2,303
Ubicación	[VID4_3N=1]	-,306	,577	,281	1	,596	-1,437	,826
	[VID4_3N=2]	-,573	,634	,417	1	,004	-1,817	,670
	[VID4_3N=3]	0[a]	.	.	0	.	.	.

Función de enlace: Logit.

a. Este parámetro está establecido en cero porque es redundante.

Los resultados en conjunto que se tiene en la tabla se muestran los coeficientes de la expresión de la regresión de la gestión de riesgos potenciales el nivel bajo (1), frente a la seguridad de la información. Al respecto la gestión de riesgos potenciales tiene al valor de Wald de 0.417; lo que quiere decir que el Programa de Desarrollo Productivo Agrario Rural cuenta con un bajo nivel de gestión de riesgos potenciales, por lo que la probabilidad de que el nivel de la seguridad de la información sea deficiente, sin embargo una buena gestión de riesgos potenciales, tiene la probalidad de que la seguridad de la información sea eficiente, siendo este significativo ya que el p_valor (0.004) < al nivel de significancia estadística (p<0.05).

Prueba de hipótesis especifica 4

Ho: La gestión del riesgo potencial de TI no influye en la seguridad de la información del Programa de Desarrollo Productivo Agrario Rural 2017.

H1: La gestión del riesgo potencial de TI influye en la seguridad de la información del Programa de Desarrollo Productivo Agrario Rural 2017.

Tabla 19

Prueba de hipótesis especifica 4

Pseudo R cuadrado	
Cox y Snell	,130
Nagelkerke	,270
McFadden	,160

Función de enlace: Logit.

En cuanto de la prueba del pseudo R cuadrado, lo que estarían presentando es la dependencia porcentual de la gestión de riesgos potenciales en la seguridad de la información, el cual tiene el coeficiente de Nagalkerke, implicando que la variabilidad de la seguridad de la información depende del 27% de la gestión de riesgos potenciales en la seguridad de la información del Programa de Desarrollo Productivo Agrario Rural 2017.

Resultado específico 5

Tabla 20

Estimación de parámetros de los salvaguardas para los riesgos de TI en la seguridad de la información del Programa de Desarrollo Productivo Agrario Rural 2017.

Estimaciones de parámetro

							Intervalo de confianza al 95%	
		Estimación	Error estándar	Wald	gl	Sig.	Límite inferior	Límite superior
Umbral	[VAR2_3N = 1]	-,067	,478	,020	1	,888	-1,004	,870
	[VAR2_3N = 2]	1,826	,510	12,798	1	,000	,826	2,827
	[VAR2_3N = 3]	1,917	,562	4,325	1	,009	2,130	1,303
Ubicación	[VID5_3N=1]	,277	,522	,282	1	,595	-,747	1,301
	[VID5_3N=2]	,423	,589	,691	1	,001	-,731	1,577
	[VID5_3N=3]	0[a]	.	.	0	.	.	.

Función de enlace: Logit.

a. Este parámetro está establecido en cero porque es redundante.

Los resultados en conjunto que se tiene en la tabla se muestran los coeficientes de la expresión de la regresión de los salvaguardas para los riesgos de TI el nivel bajo (1) frente a la seguridad de la información. Al respecto los salvaguardas para los riesgos de TI tiene al valor de Wald de 0.691; lo que quiere decir que el Programa de Desarrollo Productivo Agrario Rural cuenta con un bajo nivel de gestión de salvaguardas en los riesgos de TI, por lo que la probabilidad de que el nivel de la seguridad de la información sea deficiente, sin embargo una buena gestión de salvaguardas en los riesgos de TI tiene la probalidad de que la seguridad de la información sea eficiente, siendo este significativo ya que el p_valor es (0.001) < al nivel de significancia estadística (p<0.05).

Prueba de hipótesis especifica 5

Ho: La aplicación de salvaguardas a los riesgos de TI no influye en la seguridad de la información del Programa de Desarrollo Productivo Agrario Rural 2017.

H1: La aplicación de salvaguardas a los riesgos de TI influye en la seguridad de la información del Programa de Desarrollo Productivo Agrario Rural 2017.

Tabla 21

Prueba de hipótesis especifica 5.

Pseudo R cuadrado	
Cox y Snell	,400
Nagelkerke	,500
McFadden	,200

Función de enlace: Logit.

En cuanto de la prueba del pseudo R cuadrado, lo que estarían presentando es la dependencia porcentual de los salvaguardas de la gestión de riesgos en la seguridad de la información, el cual tiene el coeficiente de Nagalkerke, implicando que la variabilidad de la seguridad de la información depende del 50% de la los salvaguardas de la gestión de riesgos en la seguridad de la información en el Programa de Desarrollo Productivo Agrario Rural 2017.

IV. Discusión

De la tabla 06 se obtiene que de la gestión de riesgos de TI en el Programa de Desarrollo Productivo Agrario Rural 2017, el 63,33% percibe que el nivel es malo en cuanto a la gestión de riesgos, mientras que el 26,67% percibe que el nivel es regular y el 10.00% percibe que el nivel de la gestión de riesgos en Agrorural es bueno. Por lo que el nivel de la gestión de riesgos de TI en el Programa de Desarrollo Productivo Agrario Rural es malo.

De tabla 07 se aprecian los resultados generales de la seguridad de la información en el Programa de Desarrollo Productivo Agrario Rural 2017, en donde el 50,00% percibe que el nivel es deficiente en cuanto a la gestión de riesgos, mientras que el 34,17% percibe que el nivel es regular y el 15,83% percibe que el nivel de la gestión de riesgos en el Programa de Desarrollo Productivo Agrario Rural es eficiente. Lo que evidencia que el nivel de la seguridad de la información en el Programa de Desarrollo Productivo Agrario Rural es deficiente.

De la tabla 08 el valor Chi cuadrado es de 22,7 y p_valor (valor de la significancia) es igual a 0.035 frente a la significación estadística α igual a 0.05 (p_valor < α), significa rechazo de la hipótesis nula, los datos de la variable no son independientes, implica que la variable seguridad de la información depende de la variable gestión de riesgos de TI. Así mismo en la tabla 09 es posible mostrar la dependencia gracias a las variables y el modelo presentado que estaría dado por el valor estadístico Pearson de valor 0.716 frente al permitido de 0.05. Por tanto, el modelo y los resultados están explicando la dependencia de una variable sobre la otra.

Analizando luego la tabla 10. Se muestra los indicadores de la expresión de la regresión de la gestión de riesgos al nivel bajo (1) frente a la seguridad de la información del Programa de Desarrollo Productivo Agrario Rural. Al respecto la variable gestión de riesgos (dimensiones) tiene al valor de Wald de 0.200,0.420,0.570,0.165 y 0510; lo que quiere decir que el Programa de Desarrollo Productivo Agrario Rural cuenta con una baja gestión de riesgos, por lo que existe la probabilidad de que la seguridad de la información sea deficiente, es alto, sin embargo una buena gestión del riesgo tiene la probalidad de que la seguridad de la información sea eficiente, estas dependencias claro esta se regirá

de acuerdo al grado de significancia que se obtenga cuyo valor deberá ser menor que 0.05.

En la prueba de hipótesis general se rechaza la hipótesis nula como se observa en la tabla 11, presentando la dependencia porcentual de la gestión de riesgos en la seguridad de la información en un 44%.

En cuanto al resultado de la curva COR (figura 13), se observa que el área de capacidad de clasificación es un 68.1% representando un alto grado de influencia de la gestión de riesgos de TI en la seguridad de la información del Programa de Desarrollo Productivo Agrario Rural 2017.

En la tabla 12 del resultado especifico 1, el plano de activos de información de la variable gestión de riesgos tiene al valor de Wald de 0.679; lo que quiere decir que el Programa de Desarrollo Productivo Agrario Rural cuenta con un bajo nivel de gestión de riesgos de los activos informáticos por lo que la probabilidad de que el nivel de la seguridad de la información, sea deficiente, sin embargo una buena gestión del riesgo tiene la probalidad de que la seguridad de la información sea eficiente, siendo su valor de significancia de 0.031 menor al permitido de 0.05.

En la Prueba de hipótesis especifica 1 (tabla 13), el indicador de Nagalkerke, demuestra que la variable seguridad de la información depende del 36% de la gestión de riesgos de los activos informáticos del Programa de Desarrollo Productivo Agrario Rural.

En la tabla 14 del resultado especifico 2, se tiene al valor de Wald de 0.341; lo que quiere decir que el Programa de Desarrollo Productivo Agrario rural cuenta con un bajo nivel de gestión de riesgos de las amenazas de TI, por lo que lo que existe la probabilidad de que la seguridad de la información sea deficiente, sin embargo una buena gestión del riesgo de las amenazas de TI tiene la probalidad de que la seguridad de la información sea eficiente, siendo su valor de significancia de 0.009 menor al permitido de 0.05.

En cuanto de la prueba de hipótesis especifica 2 de la tabla 15 , el indicador de Nagalkerke de 0.300, implicando que la variable seguridad de la información depende del 30% de la gestión de riesgos de las amenazas de TI del Programa de Desarrollo Productivo Agrario Rural 2017.

El conjunto del resultado especifico 3 de la tabla 16, se tiene al valor de Wald de 0.644; lo que quiere decir que el Programa de Desarrollo Productivo Agrario Rural cuenta con un bajo nivel de gestión de impacto potencial de ejecución de riesgos de TI, por lo que existe la probabilidad de la seguridad de la información sea deficiente, sin embargo una buena gestión de impacto potencial de ejecución de riesgos de TI, tiene la probalidad de que la seguridad de la información sea eficiente, siendo su valor de significancia de 0.008 menor al valor estadístico permitido de 0.05.

En cuanto de la prueba de hipótesis 3 en la tabla 17, se tiene el indicador de Nagalkerke de 0.370, implicando que la variable seguridad de la información depende del 37% de la gestión de impacto potencial de riesgos de TI del Programa de Desarrollo Productivo Agrario Rural 2017.

El conjunto del resultado especifico 4 de la tabla 18, se tiene al valor de Wald de 0.417; lo que quiere decir que el Programa de Desarrollo Productivo Agrario Rural cuenta con una baja gestión de riesgos potenciales, por lo que existe la probabilidad de que el nivel de la seguridad de la información sea deficiente, sin embargo una buena gestión de riesgos potenciales, tiene la probalidad de que la seguridad de la información sea eficiente, siendo su valor de significancia de 0.004 menor al valor estadístico permitido de 0.05.

En cuanto a la prueba de hipótesis 4 de la tabla 19, el indicador Nagalkerke es de 0.270, implicando que la variable seguridad de la información depende del 27% de la gestión de riesgos potenciales en la seguridad de la información del Programa de Desarrollo Productivo Agrario Rural 2017.

El resultado especifico 5 (tabla 20), muestra el indicador de la expresión de la regresión de los salvaguardas para los riesgos de TI frente a la seguridad de la información. Al respecto los salvaguardas para los riesgos de TI tiene al valor de Wald de 0.691; lo que quiere decir que el Programa de Desarrollo Productivo Agrario Rural cuenta con una baja gestión de salvaguardas en los riesgos de TI, por lo existe la probabilidad de que el nivel de la seguridad de la información sea deficiente, sin embargo una buena gestión de salvaguardas en los riesgos de TI

tiene la probalidad de que la seguridad de la información sea eficiente, siendo el valor de significancia de 0.001 menor al valor estadístico permitido de 0.05.
En cuanto de la prueba de hipótesis 5, de la tabla 21 se tiene el indicador de Nagalkerke, implicando que la variable seguridad de la información depende del 50% de la los salvaguardas de la gestión de riesgos en la seguridad de la información en el Programa de Desarrollo Productivo Agrario Rural 2017.

Con lo que se evidencia que se tiene que primero planear un programa integral de análisis, tratamiento y administración del riesgo de TI en el Programa de Desarrollo Productivo Agrario Rural para poder implementar un eficiente sistema de seguridad de la información de acuerdo a los estándares establecidos por las ISO: 27001(SGSI) e ISO 31000 (gestión de riesgos) normados por la secretaria digital (antes ONGEI) de la PCM utilizando la metodología Magerit.

V. Conclusiones

Primera conclusión

Existe una influencia significativa de la gestión de riesgos de TI en la seguridad de la información del Programa de Desarrollo Productivo Agrario Rural 2017 de un nivel alto teniendo este un valor de significancia de 0.035 y una dependencia de la variable seguridad de información de la variable de gestión de riesgo de TI del 44%, por lo que se indica que a una buena gestión de riesgos existe la probabilidad de una eficiente seguridad de la información, pero también está presente la probabilidad de que a una mala gestión de riesgos, la seguridad de la información sea deficiente.

Segunda conclusión

Existe una influencia significativa de la administración de los activos de información en la seguridad de la información del Programa de Desarrollo Productivo Agrario Rural 2017. Siendo este relevante, dado que de los resultados estadísticos obtenidos, la variable seguridad de la información depende en un 36% de una buena gestión de riesgo de los activos de información, y que de acuerdo a lo recopilado en el instrumento de datos se obtuvo que una buena identificación y análisis de vulnerabilidades de los activos de información puede minimizar o maximizar la ejecución de potenciales amenazas de los mismos; afectando la continuidad operativa de Agrorural, por otro lado el valor de significancia de 0.031 corrobora la dependencia de la seguridad de información de la gestión de riesgos de los activos de información de TI.

Tercera conclusión

Existe una influencia significativa de la ejecución de amenazas de los activos de información en la seguridad de la información del Programa de Desarrollo Productivo Agrario Rural 2017. Siendo este relevante, dado que de los resultados estadísticos obtenidos, la variable seguridad de la información depende en un 30% de una buena gestión de riesgo de ejecución de amenazas de los activos de información, y que de acuerdo a lo recopilado en el instrumento de datos se obtuvo que un buen análisis y tratamiento de las amenazas de los activos de información puede minimizar o maximizar la ejecución de potenciales riesgos de los mismos; afectando la continuidad operativa de Agrorural, por otro lado el valor

de significancia de 0.009 corrobora la dependencia de la seguridad de información de la gestión de ejecución de amenazas de los activos de información de TI.

Cuarta conclusión

La variable seguridad de la información del Programa de Desarrollo Productivo Agrario Rural 2017, recibe una influencia significativa de la gestión de impacto potencial de la ejecución de riesgos de TI, dado que de los resultados estadísticos obtenidos, la variable seguridad de la información muestra dependencia en un 37% de la gestión de impacto potencial de ejecución de riesgo, por lo que se afirma que a una alta ejecución de un riesgo el impacto podría ser catastrófico, de la misma un buen tratamiento de ejecución de un riesgo, el impacto podría ser mínimo o nulo; afectando de manera alta o baja la continuidad operativa de Agrorural, por otro lado el valor de significancia de 0.008 corrobora la dependencia de la seguridad de información de la gestión de impacto potencial de ejecución de un riesgo de TI.

Quinta conclusión

Existe una influencia significativa de ejecución de riesgos potenciales de los activos de información en la seguridad de la información del Programa de Desarrollo Productivo Agrario Rural 2017. Siendo este relevante, dado que de los resultados estadísticos obtenidos, la variable seguridad de la información depende en un 27% de una buena gestión de ejecución de riesgo potencial de los activos de información, y que de acuerdo a lo recopilado en el instrumento de datos se obtuvo que un buen análisis y tratamiento del riesgo de los activos de información puede minimizar o maximizar la ejecución de potenciales riesgos de los mismos; afectando la continuidad operativa de Agrorural, por otro lado el valor de significancia de 0.004 corrobora la dependencia de la seguridad de información de la gestión de ejecución de riesgo potencial de los activos de información de TI.

Sexta conclusión

Existe una influencia significativa de aplicación de salvaguardas para minimizar la ejecución de riesgo en la seguridad de la información del Programa de Desarrollo Productivo Agrario Rural 2017. Siendo este relevante, dado que de los resultados estadísticos obtenidos, la variable seguridad de la información depende en un 50% de una buena gestión de aplicación de salvaguardas a los riesgos de los activos de información, y que de acuerdo a lo recopilado en el instrumento de datos se obtuvo que una adecuada gestión de salvaguardas para los activos de información puede minimizar o maximizar la ejecución de riesgos de TI en la institución; afectando la continuidad operativa de Agrorural, por otro lado el valor de significancia de 0.001 corrobora la dependencia de la variable seguridad de información, de los salvaguardas de los activos de información de TI.

VI. Recomendaciones

Primera: Implementar la gestión del riesgo de TI comenzando con el análisis de riesgos, que permite determinar la criticidad de la posibilidad de ejecución de los riesgos de TI en la organización y estimar lo que podría pasar, posterior a ello el tratamiento, que permitirá organizar la defensa concienzuda y prudente, para evitar un escenario catastrófico y al mismo tiempo estar preparados para atajar las emergencias, sobrevivir a los incidentes y seguir operando en las mejores condiciones. Por lo que es necesario tener en cuenta para esta implementación una adecuada administración de activos de información, identificar sus amenazas, minimizar la ejecución del riesgo y su impacto potencial; así como la adecuada aplicación de salvaguardas al riesgo.

Segunda: Establecer como principales objetivos de la seguridad informática: (1) Minimizar y gestionar los riesgos y detectar los posibles problemas y amenazas a la seguridad, (2) Garantizar la adecuada utilización de los recursos y de las aplicaciones del sistema, (3) Limitar las pérdidas y conseguir la adecuada recuperación del negocio en caso de un incidente de seguridad, (4) cumplir con el marco legal y con los requisitos impuestos por los proveedores y clientes en sus contratos, (5) conseguir el compromiso de la alta dirección y colaboradores de la institución para la adecuada gestión tanto del riesgo de TI y la seguridad de la información.

Tercera: Contemplar cuatro planos de actuación en seguridad de información: (1) Técnico, tanto a nivel físico como a nivel lógico, (2) base Legal, para se implanten una serie de medidas de seguridad (3) Humano, sensibilización de los empleados y directivos así como su formación básica en seguridad de la información, definición de funciones y obligaciones del personal, (4) Organizativo, definición e implantación de políticas de seguridad, planes, normas, procedimientos y buenas prácticas de actuación.

Cuarta Implementar la gestión de riesgos de TI en el Programa de Desarrollo Productivo agrario Rural, utilizando la metodología Margerit acoplada a la norma técnica peruana NTP - ISO 31000 .(Revisada, 2016). Gestión del riesgo. Principios y directrices (Primera ed.)

Quinta: Cumplir con los plazos establecidos en las normas y directivas establecidas por el gobierno electrónico de la PCM a través de su secretaria digital para no generar informalidades y sanciones a los colaboradores de Agrorural de las diferentes unidades orgánicas y a Agrorural mismo como institución.

Sexta Implementar el sistema de gestión de seguridad de información (SGSI) en el Programa de Desarrollo Productivo agrario Rural, utilizando la metodología Magerit acoplada a la norma técnica peruana NTP - ISO/ IEC 27001: 2014 Tecnología de la Información. Técnicas de seguridad. Sistemas de Gestión de seguridad de la información. Requisitos (Segunda ed.)

Séptima: Realizar seguimiento y control permanente de acuerdo a la gestión del cambio a las implementaciones de administración de riesgos de TI y al sistema de gestión de seguridad de la información.

VII. Referencias

Abril, A., Pulido, J., y Bohada, J. A. (2017). Análisis de Riesgos en Seguridad de la Información. Revista ciencia, innovación y tecnología, 1, 39-53. Recuperado de https://scholar.google.es/scholar?hl=es&as_sdt=0%2C5&as_ylo=2000&as_yhi=2017&q=amenazas+de+activos+de+tecnologia+de+la+informacion&btnG=

Agrorural. (2017). Oficina de Planificacion y Presupuesto. Lima Perú: Ministerio de Agricultura y Riego. Recuperado de: recuperado de: http://www.agrorural.gob.pe/gobierno-abierto/portal-de-transparencia-estandar/resoluciones-directorales-ejecutivas/

Albanese, D. E., Briozzo, A. E., Argañaraz, Á. A., y Vigier, H. P. (2013). Determinantes de la tercerización del servicio de información Contable en las pymes: el caso de la argentina. Revista de Administracion Mackenzie, 14(5), 201. Recuperado de http://ri.conicet.gov.ar/bitstream/handle/11336/2005/Mac-publicado.pdf?sequence=1

Alcántara, J. M., y Del Barrio García, S. (2016). Análisis del papel moderador de la cultura en el efecto del riesgo percibido sobre la aceptación de un sitio web de un destino turístico. Innovar, 26(63), 11. Recuperado de https://search.proquest.com/openview/a45ba2d0fccd6f5adbf51cbb0ff4ea6f/1?pq-origsite=gscholar&cbl=2035726

Aznar, H. (2002). Deberes éticos de la información confidencial. Revista Latina de Comunicación Social, 5(50), 0. Recuperado de: http://www.redalyc.org/pdf/819/81955012.pdf

Bertolín, J. A. (2008). Seguridad de la información. Redes, informática y sistemas de información. Madrid España Editorial Paraninfo.

Bonilla, S. M., y González, J. A. (2012). Modelo de seguridad de la información. Ingenierías USBMed, 3(1), 6-14.. Recuperado de http://revistas.usb.edu.co/index.php/IngUSBmed/article/view/259/173

Borbón Sanabria, J. S. (2013). Metodología ágil de establecimiento de sistemas de gestión de la seguridad de la información basados en ISO/IEC 27001. Revista Puente Científica, 6(1). Recuperado de http://rpuente.upbbga.edu.co/index.php/revistapuente/article/view/67/50

Caiza, C., y Santiago, N. (2015). Análisis y desarrollo de una política de seguridad de la información basado en la norma ISO 27000 para empresas de desarrollo de

software bancario en ecuador. Plan de investigación de fin de la carrera de Ingeniera de sistemas en informática y redes de información. Universidad Internacional SEK. Recuperado de: https://scholar.google.com.pe/scholar?lr=lang_es&q=La+informaci%C3%B3n+constituye+un+recurso+que+en+muchos+casos+no+se+valora+adecuadamente+por+su+intangibilidad+(situaci%C3%B3n+que+no+se+produce+con+los+equipos++inform%C3%A1ticos,+la+documentaci%C3%B3n+impresa+o+las+aplicaciones)+y,+adem%C3%A1s,+las+medidas+de+seguridad+no+c&hl=es&as_sdt=0,5&as_ylo=2013&as_yhi=2018

Calder, A., y Watkins, S. (2008). Gobierno de TI: una guía de gestión de seguridad de datos e ISO 27001 / ISO 27002. Kogan 31.

Carrasco, C. J. G., & Pérez, R. A. R. (2014). Aprender a enseñar ciencias sociales con métodos de indagación. Los estudios de caso en la formación del profesorado. REDU: Revista de Docencia Universitaria, 12(2), 38.

Delgado, J., y Marín, F. (2000). Evolución en los sistemas de gestión empresarial. Del MRP al ERP. Economía industrial, 331(1), 51-58. Recuperado de: https://s3.amazonaws.com/academia.edu.documents/40727673/Articulo_DRP.pdf?AWSAccessKeyId=AKIAIWOWYYGZ2Y53UL3A&Expires=1517524111&Signature=v55q0InfhIt%2FHbRqzhitc%2BDQOO8%3D&response-content-disposition=inline%3B%20filename%3DArticulo_DRP.pdf

Devia, G. A. V., y Pardo, C. J. (2014). Hacia un modelo para la gestión de riesgos de TI en Mi Pymes: MOGRIT. Sistemas y Telemática, 12(30), 35-48. Recuperado de http://www.redalyc.org/pdf/4115/411534000003.pdf

Estupiñan, R. (2015). Administración de riesgos ERM y la auditoría interna (Segunda ed.). Bogotá, Colombia. ECOE ediciones. Recuperado de https://books.google.com.pe/books?hl=es&lr=lang_es&id=psK4DQAAQBAJ&oi=fnd&pg=PT18&dq=Evaluaci%C3%B3n:+interpretaci%C3%B3n+de+los+valores+de+impacto+y+riesgo+residuales&ots=v3ZzRV0psz&sig=oRodqdaXQ-ETMwQCaTwL69PbsjQ#v=onepage&q&f=false

Eterovic, J., y Pagliari, G. (2011). Metodología de análisis de riesgos informáticos. Revista Técnica Administrativa, 10(1), 1. Recuperado de http://www.cyta.com.ar/ta1001/v10n1a3.htm

Fraume, M., Cristina, M., Cardona, O., Ordaz Schroder, M. G., y Barbat, H. A. (2008). La gestión financiera del riesgo desde la perspectiva de los desastres: evaluación de la exposición fiscal del estado y alternativas de instrumentos financieros de retención y transferencia del riesgo. Barcelona, España. Centro Internacional de Métodos Numéricos en Ingeniería (CIMNE).

Freitas, V. D. (2009). Análisis y evaluación del riesgo de la información: caso de estudio Universidad Simón Bolívar. Enl@ce: Revista Venezolana de Información, Tecnología y Conocimiento, 6(1). Recuperado de http://www.redalyc.org/html/823/82311100004/

Fúster, A., de la Guía, D., Hernandez, L., Montoya, F., y Muñoz, J. (2001). Técnicas criptográficas de protección de datos. Segunda ed. México editorial RA-MA

Galeano, B. J., Escobar, N., Cuartas, D., y Botero, J. C. (2015). Modelo integrado de gestión de activos hospitalarios basado en la pag. 55. Revista Ingeniería Biomédica, 9(18), 95-102. Recuperado de http://www.scielo.org.co/pdf/rinbi/v9n18/v9n18a11.pdf

García, M., Quispe, C., y Ráez, L. (2003). Mejora continua de la calidad en los procesos. Industrial Data, 6(1).

Gómez, A. (2014). Enciclopedia de la Seguridad Informática (Segunda ed.). Madrid, España: RA-MA.

Gómez, R., Pérez, D. H., Donoso, Y., y Herrera, A. (2010). Metodología y gobierno de la gestión de riesgos de tecnologías de la información. Revista de ingeniería, (31). Recuperado de http://www.redalyc.org/html/1210/121015012006/

Hernández Barros, Rafael (2015). Los riesgos de las entidades aseguradoras en el marco del Enterprise Risk Management (ERM) y el control interno. Innovar: Revista de ciencias administrativas y sociales, 61-70. Recuperado de http://www.redalyc.org/html/818/81842948006/

Inacal. (2011). Norma Técnica Peruana NTP - ISO 31000 .(Revisada 2016). Gestión del riesgo. Principios y directrices (Primera ed.). Lima, Perú: R.D. N° 032-2016-INACAL / DN.

Indecopi. (2014). Norma Técnica Peruana NTP - ISO/ IEC 27001: 2014 Tecnología de la Información. Técnicas de seguridad. Sistemas de Gestión de seguridad de la

información. Requisitos (Segunda ed.). Lima, Perú: R.0129-2014/ CNB - INDECOPI.

Jácome León, José Guillermo., Pusdá Chulde, Marco Remigio, Y Imbaquingo Esparza, Daisy Elizabeth. (2016). Fundamentos de Auditoría Informática basada en riesgos. Ibarra, Ecuador. Editorial UTN Ibarra.

Jimenez-Martin, A., Vicente, E., y Mateos, A. (2015). Safeguard selection for risk management in information systems: a fuzzy approach/Seleccion de salvaguardas en gestión del riesgo en sistemas de la información: un enfoque borroso. RISTI (Revista Iberica de Sistemas e Tecnologías de Información), (15), 83-101. Recuperado de https://scholar.google.es/scholar?hl=es&as_sdt=0%2C5&as_ylo=2000&as_yhi=2017&q=amenazas+de+activos+de+tecnologia+de+la+informacion&btnG=

Macau, R. (2004). TIC:¿ PARA QUÉ?(Funciones de las tecnologías de la información y la comunicación en las organizaciones). RUSC. Universities and Knowledge Society Journal, 1(1). Recuperado de: http://www.redalyc.org/html/780/78011256005/

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

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

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

Maiwald, E., y Miguel, E. A. (2005). Fundamentos de seguridad de redes. McGraw-Hill.

Moreno, M., y Camacho, O. E. (2011). Riesgos tecnológicos en la enseñanza de la ingeniería. Ciencia e Ingeniería. Mérida Venezuela, 43-52. Recuperado de http://erevistas.saber.ula.ve/index.php/cienciaeingenieria/article/view/3232/3140

Piattini Velthius Mario Gerardo y Del Peso Navarro Emilio. (2001). Auditoría Informática un enfoque práctico (Segunda ed.). Madrid, España: Alfa Omega - RAMA.

Roselló, M. J. P. (2004). Evolución histórica de los estudios sobre riesgos. Propuestas temáticas y metodológicas para la mejora del análisis y gestión del riesgo desde una perspectiva geográfica. Baética: Estudios de arte, geografía e historia. Málaga españa, (26), 103-128. Recuperado de https://scholar.google.es/scholar?hl=es&as_sdt=0%2C5&q=Evoluci%C3%B3n+hist%C3%B3rica+de+los+estudios+sobre+riesgos.+Propuestas+tem%C3%A1ticas+y+metodol%C3%B3gicas+para+la+mejora+del+an%C3%A1lisis+y+gesti%C3%B3n+del+riesgo+desde+una+perspectiva+geogr%C3%A1fica&btnG=

Santos, J. C. (2014). Seguridad y alta disponibilidad. Madrid, España. RA-MA Editorial.

Saurí, D., Ribas, A., Lara, A., y Pavón, D. (2010). La percepción del riesgo de inundación: experiencias de aprendizaje en la Costa Brava. Papeles de Geografía, (51-52), 269.

Younes, Moreno Diego. (2004). Panorama de las reformas del Estado y de la administración pública (Primera ed.). Bogotá, Colombia. Centro editorial Universidad del Rosario.

Zulueta, Y., Despaigne, E., y Hernández, A. (2009). La gestión de riesgos en la producción de software y la formación de profesionales de la informática: experiencias de una universidad cubana. REICIS. Revista Española de Innovación, Calidad e Ingeniería del Software, 5(3). Agrorural. (2017). Oficina de Planificación y Presupuesto. Lima Perú: Ministerio de Agricultura y Riego. Recuperado de: recuperado de: http://www.agrorural.gob.pe/gobierno-abierto/portal-de-transparencia-estandar/resoluciones-directorales-ejecutivas/

VIII. Anexos

Anexo 1: Matriz de Consistencia
Anexo 2: Matriz operacional de las variables.
Anexo 3: Instrumentos
Anexo 4: Certificado de validez de los instrumentos
Anexo 5: Matriz de datos de la prueba piloto
Anexo 6: Matriz de datos
Anexo 7: Tablas y gráficos alternos del capítulo resultados

Anexo1: Matriz de consistencia

Matriz de consistência

Título: Gestión de riesgos de TI en la seguridad de la información del Programa de Desarrollo Productivo Agrario Rural 2017
Autor: Melitón Ricardo Otoya Verástegui

Problema	Objetivos	Hipótesis	Variables e indicadores
Problema General: ¿En qué medida la gestión de riesgos de TI influye en la seguridad de la información del Programa de Desarrollo Productivo Agrario Rural 2017? **Problemas Específicos:** ¿En qué medida la gestión de riesgos de los activos de información de TI influye en la seguridad de la información del Programa de Desarrollo Productivo Agrario Rural 2017? ¿En qué medida la gestión de riesgos de las amenazas de TI influye en la seguridad de la información del Programa de Desarrollo Productivo Agrario Rural 2017? ¿En qué medida el impacto potencial de ejecución de riesgos de TI influye en la seguridad de la información del Programa de Desarrollo Productivo Agrario Rural 2017? ¿En qué medida la gestión del riesgo potencial de TI influye en la seguridad de la información del Programa de Desarrollo Productivo Agrario Rural 2017? ¿En qué medida la aplicación de salvaguardas a los riesgos de TI influyen en	**Objetivo general:** Determinar la influencia de la gestión de riesgos de TI en la seguridad de la información del Programa de Desarrollo Productivo agrario Rural 2017? **Objetivos específicos:** Identificar la influencia de la gestión de riesgos de los activos de información de TI en la seguridad de la información del Programa de Desarrollo Productivo Agrario Rural 2017. Medir la influencia de la gestión de riesgos de las amenazas de TI en la seguridad de la información del Programa de Desarrollo Productivo Agrario Rural 2017. Reconocer la influencia del impacto potencial de ejecución de riesgos de TI en la seguridad de la información del Programa de Desarrollo Productivo Agrario Rural 2017. Definir la influencia de la gestión de riesgo potencial de los activos de información de TI en la seguridad de la información del Programa de Desarrollo Productivo Agrario Rural 2017. Verificar la influencia de la aplicación de salvaguardas a los riesgos	**Hipótesis general:** La gestión de riesgos de TI influye en la seguridad de la información en el Programa de Desarrollo Productivo Agrario Rural 2017 **Hipótesis específicas:** La gestión de riesgos de activos de información de TI influye en la seguridad de la información del Programa de Desarrollo Productivo Agrario Rural 2017 La gestión de riesgos de las amenazas de TI influye en la seguridad de la información del Programa de Desarrollo Productivo Agrario Rural 2017. El impacto potencial de ejecución de riesgos de TI influye en la seguridad de la información del Programa de Desarrollo Productivo Agrario Rural 2017. La gestión del riesgo potencial de TI influye en la seguridad de la información del Programa de Desarrollo Productivo Agrario Rural 2017 La aplicación de salvaguardas a los riesgos de TI influye en la seguridad de la	**Variable 1: Gestión de riesgos**

Dimensiones	Indicadores	Ítems	Escala de medición	Niveles o rangos
X1. Activos de información	- Activos esenciales - Servicios internos - Equipamiento informático	(Item 1, item 2, item3, item 4, item 5)	1. Completamente en desacuerdo 2. En desacuerdo 3. Ni de acuerdo, ni desacuerdo 4. De acuerdo 5. Completamente De Acuerdo	Alta : 18-25 Moderada: 12-18 Baja : 5-12
X2. Amenazas.	- Identificación amenazas.	Item 6, item 7, item 8, item 9,)		Alta : 15-20 Moderada: 9-15 Baja : 4-8
X3. Impacto potencial.	- valoración - Impacto acumulado - Impacto repercutido	(item 10, Item 11, ítem12, item 13)		Alta : 15-20 Moderada: 9-15 Baja : 4-8
X4. Riesgo potencial.	- Riesgo acumulado - Riesgo repercutido	(item 14, item 15)		Alta : 7-10 Moderada: 5-7 Baja : 2-5
X5. Salvaguardas.	– Selección salvaguardas – Efectos de las salvaguardas	(item 16, item 17, item 18, item, 19, item 20, Item 21)		Alta: 22-30 Moderada: 14-22 Baja : 6-14

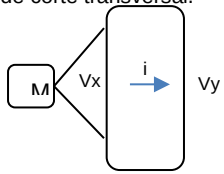
Variable 2: Seguridad de la información

Dimensiones	Indicadores	Ítems	Escala de medición	Niveles o rangos
X1. Técnico.	- Instalación - Configuración - Criptografía - Estandarización - Desarrollo de Aplicación con enfoque de seguridad	(Item 1, item 2, item3, ítem4, item 5)	1. Completamente en desacuerdo 2. En Desacuerdo 3. Ni de acuerdo, ni desacuerdo 4. De acuerdo 5. Completamente De acuerdo	Deficiente : 5-12 Regular 12-18 Eficiente 18-25
X2. Legal.	- Cumplimiento y adaptación de la legislación vigente - LSSI Firma Electrónica - Propiedad intelectual.	(Item 6, item 7, item 8)		Deficiente : 3-7 Regular: 7-11 Eficiente 11-15

<table>
<tr><th>Problema</th><th>Objetivos</th><th>Hipótesis</th><th colspan="5">Variables e indicadores</th></tr>
<tr><td>la seguridad de la información del Programa de Desarrollo Productivo Agrario Rural 2017?</td><td>de TI en la seguridad de la información del Programa de Desarrollo Productivo Agrario Rural 2017</td><td>información del Programa de Desarrollo Productivo Agrario Rural 2017.</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td>X3. Humano.</td><td>- Sensibilización y formación.
- Funciones y obligaciones
- Control y supervisión de los trabajadores</td><td>(item 9, item 10, Item 11)</td><td></td><td>Deficiente : 3-7
Regular: 7-11
Eficiente 11-15</td></tr>
<tr><td></td><td></td><td></td><td>X4. Organizativo.</td><td>- Políticas Normas Directivas Procedimientos
- Planes de Contingencia y Respuesta a Incidentes
- Relaciones con terceros (clientes, proveedores)</td><td>(ítem12, item 13, item 14, item 15,Ítem 16)</td><td></td><td>Deficiente : 5-12
Regular 12-18
Eficiente 18-25</td></tr>
<tr><th>Tipo y diseño de investigación</th><th>Población y muestra</th><th colspan="3">Técnicas e instrumentos</th><th colspan="3">Estadística a utilizar</th></tr>
<tr><td>Tipo:

Tipo Básica de nivel descriptivo con enfoque cuantitativo y de análisis Causa-efecto.

Alcance: la investigación se realizó en el Departamento de Lima distrito de Jesús María, sede central Agrorural.

Diseño: No experimental de corte transversal.
 

Dónde:
M → Muestra
Vx → Variable 1
Vy → Variable 2
I → Representa la influencia de Vx en Vy.

Método: Hipotético deductivo</td><td>Población:
La población o universo de interés en esta investigación, ésta conformada por 174 colaboradores del Programa de Desarrollo Productivo Agrario Rural, 2017.

Tipo de muestreo:
El tipo de muestreo que se utilizó fue el muestreo aleatorio simple debido a que todos los colaboradores tendrán la misma oportunidad de ser elegidos para su participación

Tamaño de muestra:
La muestra en esta investigación está conformada por 120 colaboradores del Programa de Desarrollo Productivo Agrario Rural, 2017.</td><td colspan="3">Variable 1: Gestión de Riesgos
Variable 2: Seguridad de la Información.

Tipo de instrumento:
Cuestionario de Gestión de riesgos. Año: 2017
Cuestionario de Seguridad de la información. Año: 2017

Objetivo: Determinar la influencia de la gestión de riesgos de TI en la seguridad de la información en el Programa de Desarrollo Productivo Agrario Rural 2017.
Número de ítem: 37
Aplicación: Directa
Tiempo de administración: 30 minutos
Normas de aplicación: El colaborador marcará en cada ítem conforme a lo que considere evaluado respecto de lo observado.
Escala: de Likert
Técnica: encuesta

Instrumento: cuestionario

Autor: Bach.Otoya Verástegui, Melitón Ricardo
Año: 2017
Monitoreo: realizado por el autor en el campo
Ámbito de Aplicación: Oficinas de la Sede Central Lima de Agrorural.
Forma de Administración: Manipulación directa para el levantamiento de información en el campo</td><td colspan="3">DESCRIPTIVA:
Los resultados se presentaron en cuadros de frecuencias y porcentajes con su respectiva interpretación, así como con gráficos que nos permitieron representar los datos obtenidos.

INFERENCIAL:
Se aplicó la prueba estadística causal logística ordinal que nos permitió ver si es que hay influencia entre las variables de estudio.</td></tr>
</table>

Anexo 2: Matriz operacional de las variables.

Matriz de operacionalización de la variable gestión de riesgos

Variable	Dimensiones	Indicadores	Ítems	Escala de medición	Niveles y rangos
Gestión de riesgoso	Activos de información	- Activos esenciales - Servicios internos - Equipamiento informático	- Agrorural cuenta con un inventario de activos de información en TI según la información esencial que maneja y los servicios esenciales que presta - Para el análisis de riesgos se tiene identificado los niveles o dependencias de los activos esenciales de información según la información que se maneja y los servicios prestados - Se cuenta con los servicios internos que estructuran ordenadamente el sistema de información - El equipamiento informático depende de aplicaciones(software), equipos informáticos (hardware), comunicaciones , soporte de información (cintas, discos, etc.) identificados en el inventario de activos de información de TI - Los activos precisan contar con equipamiento y suministros (energía, climatización, etcétera.) mobiliario, que está identificado y asignado a un responsable en Agrorural.	1=completamente en desacuerdo 2=En desacuerdo 3=Ni de acuerdo, ni desacuerdo 4=De acuerdo 5= Completamente de acuerdo	Alta : [18-25> Moderada: [12-18> Baja :[5-12>
	Amenazas	- Identificación amenazas - valoración	- Se ha identificado adecuadamente las amenazas de origen natural, del entorno, defectos de las aplicaciones. - Se ha identificado las amenazas causadas por personas de forma accidental - Se ha identificado amenazas causadas por personas de forma deliberada - Se ha valorizado las amenazas considerando los niveles de degradación (cuán perjudicial resultaría) y probabilidad (cuan probable o improbable es que se materialice la amenaza).		Alta : [15-20> Moderada: [9-15> Baja :[4-8>
	Impacto potencial	- Impacto acumulado - Impacto repercutido	- Se ha valorizado el impacto potencial de la materialización de la amenaza en el activo de información. - Se ha calculado el impacto acumulado, considerando su valor y el valor de los activos que dependen de él, así como, - tomando en cuenta las amenazas a las que está expuesto. - Se ha graficado el nivel de dependencia de los activos, para determinar el impacto repercutido - Se ha calculado el impacto repercutido.		Alta : [15-20> Moderada: [9-15> Baja :[4-8>
	Riesgo potencial	- Riesgo acumulado - Riesgo repercutido	- Se ha determinado el riesgo acumulado por cada activo de información - Se ha determinado el riesgo repercutido por cada activo de información		Alta : [7-10> Moderada: [5-7> Baja : [2-5>
	Salvaguardas	- Selección salvaguardas - Efectos de las salvaguardas	- Se cuenta con procedimientos, mecanismos tecnológicos (salvaguardas),que reducen el riesgo - Los servicios de terceros o subcontrata relacionados a los activos de información. Está regulado dentro de Agrorural. - El personal a cargo de los activos esenciales tiene claramente definidas sus actividades - Se ha estimado los costos de mano de obra especializada en recuperar los activos esenciales - Se cuenta con una directiva que regule las salvaguardas de los activos de información - Se tiene estimado las sanciones por incumplimiento de la ley u obligaciones contractuales		Alta: [22-30> Moderada: [14-22> Baja :[6-14>

Matriz de operacionalización de la variable seguridad de la información

Variable	Dimensiones	Indicadores	Ítems	Escala de medición	Niveles y rangos
Seguridad de la información	Técnico	- Instalación - Configuración - Criptografía - Estandarización - Desarrollo de Aplicación con - enfoque de seguridad	- La configuración de seguridad del Data Center en su opinión es adecuado para hacer frente a riesgos - En términos de infraestructura (hardware) el Data Center cuenta lo necesario para asegurar la información de AGRO RURAL? - En AGRO RURAL se cuenta con estándares de seguridad de la información - Se administra adecuadamente las identidades y accesos a los sistemas en términos de seguridad de la información - Se cuenta con una aplicación para la administración de la Seguridad de la Información	1=completamente en desacuerdo 2=En desacuerdo 3=Ni de acuerdo, ni desacuerdo 4=De acuerdo 5= Completamente de acuerdo	Deficiente :[5-12> Regular [12-18> Eficiente [18-25>
	Legal	- Cumplimiento y adaptación de la legislación vigente - LSSI Firma Electrónica - Propiedad intelectual.	- Se ha implementado las NTP ISO 27001 Seguridad de la Información? - En AGRO RURAL se cumplen con la normatividad vigente en Seguridad dela Información - En AGRO RURAL se utiliza Certificado Digital, Firma Electrónica		Deficiente : [3-7> Regular: [7-11> Eficiente [11-15>
	Humano	- Sensibilización y formación. - Funciones y obligaciones - Control y supervisión de los trabajadores	- El personal a cargo del Data Center cuenta con la formación adecuada para el cumplimiento de sus funciones - El personal es supervisado oportunamente y cuenta con controles establecidos - Se cuenta con un equipo de profesionales suficiente para las necesidades de seguridad de la información		Deficiente : [3-7> Regular: [7-11> Eficiente [11-15>
	Organizativo	- Políticas Normas Directivas Procedimientos - Planes de Contingencia y Respuesta a Incidentes - Relaciones con terceros (clientes, proveedores)	- AGRO RURAL cuenta con Política de Seguridad - Se cuenta con Directivas, procedimientos que regulan las actividades vinculadas a la seguridad de la información - Se cuenta con un Plan de Contingencia - Las incidencias son atendidas y registradas - Se administra adecuadamente a proveedores de información y clientes consumidores de la información.		Deficiente : [5-12> Regular [12-18> Eficiente {18-25>

Anexo3: Instrumentos

Cuestionario para colaboradores sede central Lima Agrorural Variable (1): Gestión de Riesgos

I. Instrucciones

Estimado(a) colaboradores Agrorural, el presente instrumento tiene la finalidad de recoger información sobre la gestión de riesgos de TI de la sede central Lima del Programa de Desarrollo Productivo agrario Rural. Le pedimos que sea sincero en sus respuestas.

II. Información específica

Estimado colaborador, marque sólo una de las opciones:

Completamente en desacuerdo	En desacuerdo	Ni desacuerdo ni de acuerdo	De acuerdo	Completamente de acuerdo
1	2	3	4	5

Nº	Ítems	1	2	3	4	5
1	Agrorural cuenta con un inventario de activos de información en TI según la información esencial que maneja y los servicios esenciales que presta					
2	Para el análisis de riesgos se tiene identificado los niveles o dependencias de los activos esenciales de información según la información que se maneja y los servicios prestados					
3	Se cuenta con los servicios internos que estructuran ordenadamente el sistema de información					
4	El equipamiento informático depende de aplicaciones(software), equipos informáticos (hardware), comunicaciones , soporte de información (cintas, discos, etc.) identificados en el inventario de activos de información de TI					
5	Los activos precisan contar con equipamiento y suministros (energía, climatización, etcétera.) mobiliario, que está identificado y asignado a un responsable en Agrorural.					
6	Se ha identificado adecuadamente las amenazas de origen natural, del entorno, defectos de las aplicaciones.					
7	Se ha identificado las amenazas causadas por personas de forma accidental					
8	Se ha identificado amenazas causadas por personas de forma deliberada					
9	Se ha valorizado las amenazas considerando los niveles de degradación (cuán perjudicial resultaría) y probabilidad (cuan probable o improbable es que se materialice la amenaza).					
10	Se ha valorizado el impacto potencial de la materialización de la amenaza en el activo de información.					
11	Se ha calculado el impacto acumulado, considerando su valor y el valor de los activos que dependen de él, así como, tomando en cuenta las amenazas a las que está expuesto.					
12	Se ha graficado el nivel de dependencia de los activos, para determinar el impacto repercutido					
13	Se ha calculado el impacto repercutido.					
14	Se ha determinado el riesgo acumulado por cada activo de información					
15	Se ha determinado el riesgo repercutido por cada activo de información					
16	Se cuenta con procedimientos, mecanismos tecnológicos (salvaguardas),que reducen el riesgo					
17	Los servicios de terceros o subcontrata relacionados a los activos de información, está regulado dentro de Agrorural.					
18	El personal a cargo de los activos esenciales tiene claramente definidas sus actividades					
19	Se ha estimado los costos de mano de obra especializada en recuperar los activos esenciales					
20	Se cuenta con una directiva que regule las salvaguardas de los activos de información					
21	Se tiene estimado las sanciones por incumplimiento de la ley u obligaciones contractuales					

Cuestionario para colaboradores sede central Lima Agrorural Variable (2): Seguridad de la Información

I. Instrucciones

Estimado(a) colaboradores, el presente instrumento tiene la finalidad de recoger información sobre la seguridad de la información de la sede central Lima del Programa de Desarrollo Productivo agrario Rural. Le pedimos que sea sincero en sus respuestas.

II. Información específica

Estimado colaborador, marque sólo una de las opciones:

Completamente en desacuerdo	En desacuerdo	Ni desacuerdo ni deacuerdo	De acuerdo	Completamente de acuerdo
1	2	3	4	5

Nº	Ítems	1	2	3	4	5
1	La configuración de seguridad del Data Center en su opinión es adecuado para hacer frente a riesgos					
2	En términos de infraestructura (hardware) el Data Center cuenta lo necesario para asegurar la información de AGRO RURAL					
3	En AGRO RURAL se cuenta con estándares de seguridad de la información					
4	Se administra adecuadamente las identidades y accesos a los sistemas en términos de seguridad de la información					
5	Se cuenta con una aplicación para la administración de la Seguridad de la Información					
6	Se ha implementado las NTP ISO 27001 Seguridad de la Información?					
7	En AGRO RURAL se cumplen con la normatividad vigente en Seguridad dela Información					
8	En AGRO RURAL se utiliza Certificado Digital, Firma Electrónica					
9	El personal a cargo del Data Center cuenta con la formación adecuada para el cumplimiento de sus funciones					
10	El personal es supervisado oportunamente y cuenta con controles establecidos					
11	Se cuenta con un equipo de profesionales suficiente para las necesidades de seguridad de la información					
12	AGRO RURAL cuenta con Política de Seguridad					
13	Se cuenta con Directivas, procedimientos que regulan las actividades vinculadas a la seguridad de la información					
14	Se cuenta con un Plan de Contingencia					
15	Las incidencias son atendidas y registradas					

Anexo4: Certificado de validez de los instrumentos

CERTIFICADO DE VALIDEZ DE CONTENDO DEL INSTRUMENTO QUE MIDE LA GESTIÓN DE RIESGOS

Nº	DIMENSIONES / items	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
	I. ACTIVOS DE INFORMACION	**Si**	**No**	**Si**	**No**	**Si**	**No**	
1	Agrorural cuenta con un inventario de activos de información en TI según la información esencial que maneja y los servicios esenciales que presta							
2	Para el análisis de riesgos se tiene identificado los niveles o dependencias de los activos esenciales de información según la información que se maneja y los servicios prestados							
3	Se cuenta con los servicios internos que estructuran ordenadamente el sistema de información							
4	El equipamiento informático depende de aplicaciones(software), equipos informáticos (hardware), comunicaciones , soporte de información (cintas, discos, etc.) identificados en el inventario de activos de información de TI							
5	Los activos precisan contar con equipamiento y suministros (energía, climatización, etcétera.) mobiliario, que está identificado y asignado a un responsable en Agrorural.							
	II. AMENAZAS	**Si**	**No**	**Si**	**No**	**Si**	**No**	
6	Se ha identificado adecuadamente las amenazas de origen natural, del entorno, defectos de las aplicaciones.							
7	Se ha identificado las amenazas causadas por personas de forma accidental							
8	Se ha identificado amenazas causadas por personas de forma deliberada							
9	Se ha valorizado las amenazas considerando los niveles de degradación (cuán perjudicial resultaría) y probabilidad (cuan probable o improbable es que se materialice la amenaza).							
	III. IMPACTO POTENCIAL	**Si**	**No**	**Si**	**No**	**Si**	**No**	
10	Se ha valorizado el impacto potencial de la materialización de la amenaza en el activo de información.							
11	Se ha calculado el impacto acumulado, considerando su valor y el valor de los activos que dependen de él, así como, tomando en cuenta las amenazas a las que está expuesto.							
12	Se ha graficado el nivel de dependencia de los activos, para determinar el impacto repercutido							
13	Se ha calculado el impacto repercutido.							
	IV. RIESGO POTENCIAL	**Si**	**No**	**Si**	**No**	**Si**	**No**	

Nº	DIMENSIONES / items	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
14	Se ha determinado el riesgo acumulado por cada activo de información							
15	Se ha determinado el riesgo repercutido por cada activo de información							
	V. SALVAGUARDAS	**Si**	**No**	**Si**	**No**	**Si**	**No**	
16	Se cuenta con procedimientos, mecanismos tecnológicos (salvaguardas),que reducen el riesgo							
17	Los servicios de terceros o subcontrata relacionados a los activos de información. Está regulado dentro de Agrorural.							
18	El personal a cargo de los activos esenciales tiene claramente definidas sus actividades							
19	Se ha estimado los costos de mano de obra especializada en recuperar los activos esenciales							
20	Se cuenta con una directiva que regule las salvaguardas de los activos de información							
21	Se tiene estimado las sanciones por incumplimiento de la ley u obligaciones contractuales							

Observaciones (precisar si hay suficiencia):_____

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

Apellidos y nombres del juez validador. Dr/ Mg**: …… DNI:……**

Especialidad del validador:……

…….de……..del 20…..

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

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

---

Firma del Experto Informante.

CERTIFICADO DE VALIDEZ DE CONTENDO DEL INSTRUMENTO QUE MIDE LA SEGURIDAD DE LA INFORMACION

Nº	DIMENSIONES / ítems	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
	I. TECNICO	**Si**	**No**	**Si**	**No**	**Si**	**No**	
1	La configuración de seguridad del Data Center en su opinión es adecuado para hacer frente a riesgos							
2	En términos de infraestructura (hardware) el Data Center cuenta lo necesario para asegurar la información de AGRO RURAL?							
3	En AGRO RURAL se cuenta con estándares de seguridad de la información							
4	Se administra adecuadamente las identidades y accesos a los sistemas en términos de seguridad de la información							
5	Se cuenta con una aplicación para la administración de la Seguridad de la Información							
	II. LEGAL	**Si**	**No**	**Si**	**No**	**Si**	**No**	
6	Se ha implementado las NTP ISO 27001 Seguridad de la Información?							
7	En AGRO RURAL se cumplen con la normatividad vigente en Seguridad dela Información							
8	En AGRO RURAL se utiliza Certificado Digital, Firma Electrónica							
	III. HUMANO	**Si**	**No**	**Si**	**No**	**Si**	**No**	
9	El personal a cargo del Data Center cuenta con la formación adecuada para el cumplimiento de sus funciones							
10	El personal es supervisado oportunamente y cuenta con controles establecidos							
11	Se cuenta con un equipo de profesionales suficiente para las necesidades de seguridad de la información							
	IV. ORGANIZATIVO	**Si**	**No**	**Si**	**No**	**Si**	**No**	
12	AGRO RURAL cuenta con Política de Seguridad							
13	Se cuenta con Directivas, procedimientos que regulan las actividades vinculadas a la seguridad de la información							
14	Se cuenta con un Plan de Contingencia							
15	Las incidencias son atendidas y registradas							
16	Se administra adecuadamente a proveedores de información y clientes consumidores de la información.							

Observaciones (precisar si hay suficiencia):_____

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

Apellidos y nombres del juez validador. Dr/ Mg**: …… DNI:……**

Especialidad del validador:……

…….de……..del 20…..

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

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

---

Firma del Experto Informante.

UCV
UNIVERSIDAD CÉSAR VALLEJO
ESCUELA DE POSTGRADO

CERTIFICADO DE VALIDEZ DE CONTENDO DEL INSTRUMENTO QUE MIDE LA GESTIÓN DE RIESGOS

N°	DIMENSIONES / ítems	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
	I. ACTIVOS DE INFORMACION	Si	No	Si	No	Si	No	
1	Agrorural cuenta con un inventario de activos de información en TI según la información esencial que maneja y los servicios esenciales que presta	✓		✓		✓		
2	Para el análisis de riesgos se tiene identificado los niveles o dependencias de los activos esenciales de información según la información que se maneja y los servicios prestados	✓		✓		✓		
3	Se cuenta con los servicios internos que estructuran ordenadamente el sistema de información	✓		✓		✓		
4	El equipamiento informático depende de aplicaciones(software), equipos informáticos (hardware), comunicaciones , soporte de información (cintas, discos, etc.) identificados en el inventario de activos de información de TI	✓		✓		✓		
5	Los activos precisan contar con equipamiento y suministros (energía, climatización, etcétera.) mobiliario, que está identificado y asignado a un responsable en Agrorural.	✓		✓		✓		
	II. AMENAZAS	Si	No	Si	No	Si	No	
6	Se ha identificado adecuadamente las amenazas de origen natural, del entorno, defectos de las aplicaciones.	✓		✓		✓		
7	Se ha identificado las amenazas causadas por personas de forma accidental	✓		✓		✓		
8	Se ha identificado amenazas causadas por personas de forma deliberada	✓		✓		✓		
9	Se ha valorizado las amenazas considerando los niveles de degradación (cuán perjudicial resultaría) y probabilidad (cuan probable o improbable es que se materialice la amenaza).	✓		✓		✓		
	III. IMPACTO POTENCIAL	Si	No	Si	No	Si	No	
10	Se ha valorizado el impacto potencial de la materialización de la amenaza en el activo de información.	✓		✓		✓		
11	Se ha calculado el impacto acumulado, considerando su valor y el valor de los activos que dependen de él, así como, tomando en cuenta las amenazas a las que está expuesto.	✓		✓		✓		
12	Se ha graficado el nivel de dependencia de los activos, para determinar el impacto repercutido	✓		✓		✓		
13	Se ha calculado el impacto repercutido.	✓		✓		✓		
	IV. RIESGO POTENCIAL	Si	No	Si	No	Si	No	
14	Se ha determinado el riesgo acumulado por cada activo de	✓		✓		✓		

Nº	DIMENSIONES / ítems	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
	información							
15	Se ha determinado el riesgo repercutido por cada activo de información	✓		✓		✓		
	V. SALVAGUARDAS	Si	No	Si	No	Si	No	
16	Se cuenta con procedimientos, mecanismos tecnológicos (salvaguardas),que reducen el riesgo	✓		✓		✓		
17	Los servicios de terceros o subcontrata relacionados a los activos de información. Está regulado dentro de Agrorural.	✓		✓		✓		
18	El personal a cargo de los activos esenciales tiene claramente definidas sus actividades	✓		✓		✓		
19	Se ha estimado los costos de mano de obra especializada en recuperar los activos esenciales	✓		✓		✓		
20	Se cuenta con una directiva que regule las salvaguardas de los activos de información	✓		✓		✓		
21	Se tiene estimado las sanciones por incumplimiento de la ley u obligaciones contractuales	✓		✓		✓		

Observaciones (precisar si hay suficiencia): Si hay suficiencia

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

Apellidos y nombres del juez validador Dr/ Mg: Flores Sotelo Willian Sebastian **DNI:** 06175729

Especialidad del validador: Gestion Economica empresarial / Economia.

26 de Nov. del 20 17

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

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

Firma del Experto Informante.

Dr. Willian Sebastian Flores Sotelo
Docente Investigador de Posgrado
CEL N° 09426

UCV UNIVERSIDAD CÉSAR VALLEJO
ESCUELA DE POSTGRADO

CERTIFICADO DE VALIDEZ DE CONTENDO DEL INSTRUMENTO QUE MIDE LA GESTIÓN DE RIESGOS

Nº	DIMENSIONES / ítems	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
	I. ACTIVOS DE INFORMACION	Si	No	Si	No	Si	No	
1	Agrorural cuenta con un inventario de activos de información en TI según la información esencial que maneja y los servicios esenciales que presta	✓		✓		✓		
2	Para el análisis de riesgos se tiene identificado los niveles o dependencias de los activos esenciales de información según la información que se maneja y los servicios prestados	✓		✓		✓		
3	Se cuenta con los servicios internos que estructuran ordenadamente el sistema de información	✓		✓		✓		
4	El equipamiento informático depende de aplicaciones(software), equipos informáticos (hardware), comunicaciones , soporte de información (cintas, discos, etc.) identificados en el inventario de activos de información de TI	✓		✓		✓		
5	Los activos precisan contar con equipamiento y suministros (energía, climatización, etcétera.) mobiliario, que está identificado y asignado a un responsable en Agrorural.	✓		✓		✓		
	II. AMENAZAS	Si	No	Si	No	Si	No	
6	Se ha identificado adecuadamente las amenazas de origen natural, del entorno, defectos de las aplicaciones.	✓		✓		✓		
7	Se ha identificado las amenazas causadas por personas de forma accidental	✓		✓		✓		
8	Se ha identificado amenazas causadas por personas de forma deliberada	✓		✓		✓		
9	Se ha valorizado las amenazas considerando los niveles de degradación (cuán perjudicial resultaría) y probabilidad (cuan probable o improbable es que se materialice la amenaza).	✓		✓		✓		
	III. IMPACTO POTENCIAL	Si	No	Si	No	Si	No	
10	Se ha valorizado el impacto potencial de la materialización de la amenaza en el activo de información.	✓		✓		✓		
11	Se ha calculado el impacto acumulado, considerando su valor y el valor de los activos que dependen de él, así como, tomando en cuenta las amenazas a las que está expuesto.	✓		✓		✓		
12	Se ha graficado el nivel de dependencia de los activos, para determinar el impacto repercutido	✓		✓		✓		
13	Se ha calculado el impacto repercutido.	✓		✓		✓		
	IV. RIESGO POTENCIAL	Si	No	Si	No	Si	No	
14	Se ha determinado el riesgo acumulado por cada activo de	✓		✓		✓		

Nº	DIMENSIONES / ítems	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
	información							
15	Se ha determinado el riesgo repercutido por cada activo de información	✓		✓		✓		
	V. SALVAGUARDAS	**Si**	**No**	**Si**	**No**	**Si**	**No**	
16	Se cuenta con procedimientos, mecanismos tecnológicos (salvaguardas),que reducen el riesgo	✓		✓		✓		
17	Los servicios de terceros o subcontrata relacionados a los activos de información. Está regulado dentro de Agrorural.	✓		✓		✓		
18	El personal a cargo de los activos esenciales tiene claramente definidas sus actividades	✓		✓		✓		
19	Se ha estimado los costos de mano de obra especializada en recuperar los activos esenciales	✓		✓		✓		
20	Se cuenta con una directiva que regule las salvaguardas de los activos de información	✓		✓		✓		
21	Se tiene estimado las sanciones por incumplimiento de la ley u obligaciones contractuales	✓		✓		✓		

Observaciones (precisar si hay suficiencia): hay suficiencia

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

Apellidos y nombres del juez validador. Dr/ Mg: Jesús Emilio Agustin Padilla Caballero **DNI:** 25861074

Especialidad del validador: Temático y Metodologo

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

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

27 de 11 del 2017

Dr. Jesús Emilio Agustin Padilla Caballero
CPPe 0125861074
Firma del Experto Informante.

UCV UNIVERSIDAD CÉSAR VALLEJO
ESCUELA DE POSTGRADO

CERTIFICADO DE VALIDEZ DE CONTENDO DEL INSTRUMENTO QUE MIDE LA GESTIÓN DE RIESGOS

Nº	DIMENSIONES / ítems	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
	I. ACTIVOS DE INFORMACION	Si	No	Si	No	Si	No	
1	Agrorural cuenta con un inventario de activos de información en TI según la información esencial que maneja y los servicios esenciales que presta	✓		✓		✓		
2	Para el análisis de riesgos se tiene identificado los niveles o dependencias de los activos esenciales de información según la información que se maneja y los servicios prestados	✓		✓		✓		
3	Se cuenta con los servicios internos que estructuran ordenadamente el sistema de información	✓		✓		✓		
4	El equipamiento informático depende de aplicaciones(software), equipos informáticos (hardware), comunicaciones , soporte de información (cintas, discos, etc.) identificados en el inventario de activos de información de TI	✓		✓		✓		
5	Los activos precisan contar con equipamiento y suministros (energía, climatización, etcétera.) mobiliario, que está identificado y asignado a un responsable en Agrorural.	✓		✓		✓		
	II. AMENAZAS	Si	No	Si	No	Si	No	
6	Se ha identificado adecuadamente las amenazas de origen natural, del entorno, defectos de las aplicaciones.	✓		✓		✓		
7	Se ha identificado las amenazas causadas por personas de forma accidental	✓		✓		✓		
8	Se ha identificado amenazas causadas por personas de forma deliberada	✓		✓		✓		
9	Se ha valorizado las amenazas considerando los niveles de degradación (cuán perjudicial resultaría) y probabilidad (cuan probable o improbable es que se materialice la amenaza).	✓		✓		✓		
	III. IMPACTO POTENCIAL	Si	No	Si	No	Si	No	
10	Se ha valorizado el impacto potencial de la materialización de la amenaza en el activo de información.	✓		✓		✓		
11	Se ha calculado el impacto acumulado, considerando su valor y el valor de los activos que dependen de él, así como, tomando en cuenta las amenazas a las que está expuesto.	✓		✓		✓		
12	Se ha graficado el nivel de dependencia de los activos, para determinar el impacto repercutido	✓		✓		✓		
13	Se ha calculado el impacto repercutido.	✓		✓		✓		
	IV. RIESGO POTENCIAL	Si	No	Si	No	Si	No	
14	Se ha determinado el riesgo acumulado por cada activo de	✓		✓		✓		

Nº	DIMENSIONES / ítems	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
	información							
15	Se ha determinado el riesgo repercutido por cada activo de información	✓		✓		✓		
	V. SALVAGUARDAS	Si	No	Si	No	Si	No	
16	Se cuenta con procedimientos, mecanismos tecnológicos (salvaguardas),que reducen el riesgo	✓		✓		✓		
17	Los servicios de terceros o subcontrata relacionados a los activos de información. Está regulado dentro de Agrorural.	✓		✓		✓		
18	El personal a cargo de los activos esenciales tiene claramente definidas sus actividades	✓		✓		✓		
19	Se ha estimado los costos de mano de obra especializada en recuperar los activos esenciales	✓		✓		✓		
20	Se cuenta con una directiva que regule las salvaguardas de los activos de información	✓		✓		✓		
21	Se tiene estimado las sanciones por incumplimiento de la ley u obligaciones contractuales	✓		✓		✓		

Observaciones (precisar si hay suficiencia): HAY SUFICIENCIA

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

Apellidos y nombres del juez validador. Dr/ Mg: RICARDO GUEVARA FERNANDEZ **DNI:** 01048544

Especialidad del validador: METODÓLOGO – ESTADÍSTICO

27 de 11 del 2018

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

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

Dr. Ricardo Guevara Fernández
METODÓLOGO - ESTADÍSTICO
Firma del Experto Informante.

UCV UNIVERSIDAD CÉSAR VALLEJO
ESCUELA DE POSTGRADO

CERTIFICADO DE VALIDEZ DE CONTENDO DEL INSTRUMENTO QUE MIDE LA SEGURIDAD DE LA INFORMACION

Nº	DIMENSIONES / ítems	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
	I. TECNICO	**Si**	**No**	**Si**	**No**	**Si**	**No**	
1	La configuración de seguridad del Data Center en su opinión es adecuado para hacer frente a riesgos	V		V		V		
2	En términos de infraestructura (hardware) el Data Center cuenta lo necesario para asegurar la información de AGRO RURAL?	V		V		V		
3	En AGRO RURAL se cuenta con estándares de seguridad de la información	V		V		V		
4	Se administra adecuadamente las identidades y accesos a los sistemas en términos de seguridad de la información	V		V		V		
5	Se cuenta con una aplicación para la administración de la Seguridad de la Información	V		V		V		
	II. LEGAL	**Si**	**No**	**Si**	**No**	**Si**	**No**	
6	Se ha implementado las NTP ISO 27001 Seguridad de la Información?	V		V		V		
7	En AGRO RURAL se cumplen con la normatividad vigente en Seguridad dela Información	V		V		V		
8	En AGRO RURAL se utiliza Certificado Digital, Firma Electrónica	V		V		V		
	III. HUMANO	**Si**	**No**	**Si**	**No**	**Si**	**No**	
9	El personal a cargo del Data Center cuenta con la formación adecuada para el cumplimiento de sus funciones	V		V		V		
10	El personal es supervisado oportunamente y cuenta con controles establecidos	V		V		V		
11	Se cuenta con un equipo de profesionales suficiente para las necesidades de seguridad de la información	V		V		V		
	IV. ORGANIZATIVO	**Si**	**No**	**Si**	**No**	**Si**	**No**	
12	AGRO RURAL cuenta con Política de Seguridad	V		V		V		
13	Se cuenta con Directivas, procedimientos que regulan las actividades vinculadas a la seguridad de la información	V		V		V		

Nº	DIMENSIONES / ítems	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
14	Se cuenta con un Plan de Contingencia	√		√		√		
15	Las incidencias son atendidas y registradas	√		√		√		
16	Se administra adecuadamente a proveedores de información y clientes consumidores de la información.	√		√		√		

Observaciones (precisar si hay suficiencia): Si hay suficiencia.

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

Apellidos y nombres del juez validador. Dr/ Mg: Flores Sotelo William **DNI:** 06175729

Especialidad del validador: Gestión económica empresarial / Economía

26 de NOV del 2017

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

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

----
Firma del Experto Informante.

Dr. William Sebastián Flores Sotelo
Docente Investigador de Posgrado
CEL Nº 09426

UCV
Universidad César Vallejo
ESCUELA DE POSTGRADO

CERTIFICADO DE VALIDEZ DE CONTENDO DEL INSTRUMENTO QUE MIDE LA SEGURIDAD DE LA INFORMACION

Nº	DIMENSIONES / ítems	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
	I. TECNICO	**Si**	**No**	**Si**	**No**	**Si**	**No**	
1	La configuración de seguridad del Data Center en su opinión es adecuado para hacer frente a riesgos	✓		✓		✓		
2	En términos de infraestructura (hardware) el Data Center cuenta lo necesario para asegurar la información de AGRO RURAL?	✓		✓		✓		
3	En AGRO RURAL se cuenta con estándares de seguridad de la información	✓		✓		✓		
4	Se administra adecuadamente las identidades y accesos a los sistemas en términos de seguridad de la información	✓		✓		✓		
5	Se cuenta con una aplicación para la administración de la Seguridad de la Información	✓		✓		✓		
	II. LEGAL	**Si**	**No**	**Si**	**No**	**Si**	**No**	
6	Se ha implementado las NTP ISO 27001 Seguridad de la Información?	✓		✓		✓		
7	En AGRO RURAL se cumplen con la normatividad vigente en Seguridad dela Información	✓		✓		✓		
8	En AGRO RURAL se utiliza Certificado Digital, Firma Electrónica	✓		✓		✓		
	III. HUMANO	**Si**	**No**	**Si**	**No**	**Si**	**No**	
9	El personal a cargo del Data Center cuenta con la formación adecuada para el cumplimiento de sus funciones	✓		✓		✓		
10	El personal es supervisado oportunamente y cuenta con controles establecidos	✓		✓		✓		
11	Se cuenta con un equipo de profesionales suficiente para las necesidades de seguridad de la información	✓		✓		✓		
	IV. ORGANIZATIVO	**Si**	**No**	**Si**	**No**	**Si**	**No**	
12	AGRO RURAL cuenta con Política de Seguridad	✓		✓		✓		
13	Se cuenta con Directivas, procedimientos que regulan las actividades vinculadas a la seguridad de la información	✓		✓		✓		

Nº	DIMENSIONES / ítems	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
14	Se cuenta con un Plan de Contingencia	✓		✓		✓		
15	Las incidencias son atendidas y registradas	✓		✓		✓		
16	Se administra adecuadamente a proveedores de información y clientes consumidores de la información.	✓		✓		✓		

Observaciones (precisar si hay suficiencia): hay suficiencia

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

Apellidos y nombres del juez validador. Dr/ Mg: Jesús Emilio Agustín Padilla Caballero **DNI:** 25861074

Especialidad del validador: Temático y Metodologo

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

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

27 de 11 del 2017

Dr. Jesús Emilio Agustín Padilla Caballero
CPP. 0125861074

Firma del Experto Informante.

UCV UNIVERSIDAD CÉSAR VALLEJO
ESCUELA DE POSTGRADO

CERTIFICADO DE VALIDEZ DE CONTENDO DEL INSTRUMENTO QUE MIDE LA SEGURIDAD DE LA INFORMACION

Nº	DIMENSIONES / ítems	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
	I. TECNICO	**Si**	**No**	**Si**	**No**	**Si**	**No**	
1	La configuración de seguridad del Data Center en su opinión es adecuado para hacer frente a riesgos	V		V		V		
2	En términos de infraestructura (hardware) el Data Center cuenta lo necesario para asegurar la información de AGRO RURAL?	V		V		V		
3	En AGRO RURAL se cuenta con estándares de seguridad de la información	V		V		V		
4	Se administra adecuadamente las identidades y accesos a los sistemas en términos de seguridad de la información	V		V		V		
5	Se cuenta con una aplicación para la administración de la Seguridad de la Información	V		V		V		
	II. LEGAL	**Si**	**No**	**Si**	**No**	**Si**	**No**	
6	Se ha implementado las NTP ISO 27001 Seguridad de la Información?	V		V		V		
7	En AGRO RURAL se cumplen con la normatividad vigente en Seguridad dela Información	V		V		V		
8	En AGRO RURAL se utiliza Certificado Digital, Firma Electrónica	V		V		V		
	III. HUMANO	**Si**	**No**	**Si**	**No**	**Si**	**No**	
9	El personal a cargo del Data Center cuenta con la formación adecuada para el cumplimiento de sus funciones	V		V		V		
10	El personal es supervisado oportunamente y cuenta con controles establecidos	V		V		V		
11	Se cuenta con un equipo de profesionales suficiente para las necesidades de seguridad de la información	V		V		V		
	IV. ORGANIZATIVO	**Si**	**No**	**Si**	**No**	**Si**	**No**	
12	AGRO RURAL cuenta con Política de Seguridad	V		V		V		
13	Se cuenta con Directivas, procedimientos que regulan las actividades vinculadas a la seguridad de la información	V		V		V		

Nº	DIMENSIONES / ítems	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
14	Se cuenta con un Plan de Contingencia	✓		✓		✓		
15	Las incidencias son atendidas y registradas	✓		✓		✓		
16	Se administra adecuadamente a proveedores de información y clientes consumidores de la información.	✓		✓		✓		

Observaciones (precisar si hay suficiencia): HAY SUFICIENCIA

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

Apellidos y nombres del juez validador. Dr/ Mg: RICARDO GUEVARA FERNANDEZ **DNI:** 01048544

Especialidad del validador: METODÓLOGO - ESTADÍSTICO

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

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

27 de 11 del 2018

Dr. Ricardo Guevara Fernández
METODÓLOGO - ESTADÍSTICO
Firma del Experto Informante.

Anexo 5: Matriz de datos de la prueba piloto

MATRIZ DE DATOS DE LA VARIABLE GESTION DE RIESGOS																						MATRIZ DE DATOS DE LA VARIABLE SEGURIDAD DE LA INFORMACION																	
	Activos de información					Amenazas				Impacto potencial				Riesgo potencial		Salvaguardas					V1	Técnico					Legal			Humano			Organizativo					V2
Nº	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	T	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	T
1	1	1	2	1	2	3	2	1	1	2	2	2	2	4	3	2	3	1	2	2	3	42	4	4	1	4	2	2	5	5	5	5	2	2	3	2	5	3	54
2	1	2	4	1	4	3	1	1	4	1	2	4	3	2	1	3	2	4	3	1	1	48	2	2	1	1	4	4	1	5	2	1	2	3	4	1	4	2	39
3	3	5	3	5	2	4	5	5	2	5	2	4	3	5	5	2	5	5	5	2	4	81	3	5	3	3	3	1	1	3	5	2	1	3	2	2	1	1	39
4	3	1	1	3	2	2	1	4	1	3	3	4	1	1	1	1	1	4	2	3	4	46	1	2	1	2	1	1	2	3	4	4	5	4	1	3	2	1	37
5	5	1	2	2	1	2	2	1	3	1	2	1	3	1	1	4	3	2	4	3	2	46	3	3	3	3	5	1	2	1	5	1	1	2	1	1	5	2	39
6	2	5	2	5	1	2	5	2	1	1	1	1	4	4	2	1	1	2	1	4	1	48	3	1	2	4	2	3	1	3	3	4	1	1	3	3	1	1	36
7	5	4	1	1	1	1	1	2	4	1	1	3	3	3	2	1	2	1	1	2	1	41	4	4	4	1	2	1	2	1	1	1	2	3	4	5	3	2	40
8	4	2	2	5	5	1	1	1	1	1	2	1	1	3	4	3	1	2	1	4	2	47	4	3	2	1	1	5	1	3	5	3	1	2	5	2	2	2	42
9	3	3	2	2	4	2	3	2	5	5	5	5	5	5	5	4	5	4	4	3	4	80	1	1	5	2	2	3	1	1	2	1	5	3	5	2	2	4	40
10	4	3	1	4	2	2	2	5	2	1	4	2	2	3	3	1	1	1	1	1	1	46	3	3	3	2	5	5	5	3	3	5	5	4	4	3	3	5	61
11	2	2	3	3	1	1	1	3	1	2	2	2	2	2	1	1	2	3	3	2	3	42	3	2	1	1	2	1	1	5	5	5	3	1	1	1	4	1	37
12	1	4	5	3	3	4	3	5	4	3	5	5	5	5	1	5	5	5	5	4	2	82	5	3	3	4	4	3	3	5	5	5	4	4	3	3	2	5	61
13	3	2	3	2	3	2	1	4	1	1	4	1	4	5	1	2	1	1	2	3	2	48	1	1	1	3	2	2	1	4	5	2	1	2	4	4	2	1	36
14	5	3	5	3	3	2	5	3	4	5	4	5	2	3	5	3	5	4	4	5	4	82	3	3	3	2	5	3	1	2	2	1	1	3	5	4	3	4	45
15	5	1	1	1	1	1	2	1	1	1	2	1	3	2	2	1	1	1	4	1	1	34	2	1	1	2	1	2	1	3	3	2	2	4	1	4	2	3	34
16	3	4	1	1	2	3	1	1	2	2	5	1	4	1	1	1	3	2	5	4	1	48	4	3	1	4	3	3	5	3	1	5	2	3	3	2	2	3	47
17	3	2	5	2	5	4	5	5	3	3	4	3	5	5	4	5	5	3	5	3	3	82	2	2	4	2	4	1	4	2	1	1	4	4	1	3	2	2	39

18	3	2	2	3	1	2	3	3	2	2	1	2	1	2	2	1	2	3	4	2	5	48	2	5	5	1	1	3	5	1	1	1	1	2	1	3	2	4	38
19	4	4	1	1	2	1	1	1	3	1	3	3	2	2	3	1	2	2	1	1	1	40	1	5	2	5	1	1	3	4	2	3	1	2	1	1	3	1	36
20	4	5	3	2	5	2	1	2	2	1	1	3	1	3	2	2	1	3	3	1	1	48	1	2	5	3	5	1	1	1	1	5	2	1	1	3	5	1	38
21	5	4	2	3	2	3	5	4	5	3	4	4	4	5	4	3	5	5	4	2	5	81	2	1	1	4	2	3	1	1	1	2	5	5	3	4	2	2	39
22	3	5	1	4	3	1	1	4	2	1	1	1	3	1	2	2	1	2	4	1	5	48	1	3	1	3	2	1	2	4	5	1	2	3	1	3	3	2	37
23	5	2	4	3	2	2	5	1	5	5	5	1	5	5	5	3	5	4	5	4	5	81	4	1	2	1	2	2	2	3	3	2	3	2	1	3	4	3	38
24	4	5	5	2	3	1	5	2	4	1	1	1	1	1	2	2	3	1	1	1	2	48	1	1	4	4	5	5	4	2	1	2	3	1	1	1	1	1	37

Anexo6: Matriz de datos

VARIABLE: GESTION DE RIESGOS																					VARIABLE: SEGURIDAD DE LA INFORMACION																											
	Activos de información					Amenazas				Impacto potencial				Riesgo potencial	Salvaguardas							Técnico								Legal	Humano				Organizativo				V1	D1	D2	D3	D4	D5	V2	D1	D2	D3	D4
Nº	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	T						T				
1	1	1	2	1	2	3	2	1	1	2	2	2	2	4	3	2	3	1	2	2	3	4	4	1	4	2	2	5	5	5	5	2	2	3	2	5	3	42	7	7	8	7	13	54	15	12	12	15
2	1	2	4	1	4	3	1	1	4	1	2	4	3	2	1	3	2	4	3	1	1	2	2	1	1	4	4	1	5	2	1	2	3	4	1	4	2	48	12	9	10	3	14	39	10	10	5	14
3	3	5	3	5	2	4	5	5	2	5	2	4	3	5	5	2	5	5	5	2	4	3	5	3	3	3	1	1	3	5	2	1	3	2	2	1	1	81	18	16	14	10	23	39	17	5	8	9
4	3	1	1	3	2	2	1	4	1	3	3	4	1	1	1	1	1	4	2	3	4	1	2	1	2	1	1	2	3	4	4	5	4	1	3	2	1	46	10	8	11	2	15	37	7	6	13	11
5	5	1	2	2	1	2	2	1	3	1	2	1	3	1	1	4	3	2	4	3	2	3	3	3	3	5	1	2	1	5	1	1	2	1	1	5	2	46	11	8	7	2	18	39	17	4	7	11
6	2	5	2	5	1	2	5	2	1	1	1	1	4	4	2	1	1	2	1	4	1	3	1	2	4	2	3	1	3	3	4	1	1	3	3	1	1	48	15	10	7	6	10	36	12	7	8	9
7	5	4	1	1	1	1	1	2	4	1	1	3	3	3	2	1	2	1	1	2	1	4	4	4	1	2	1	2	1	1	1	2	3	4	5	3	2	41	12	8	8	5	8	40	15	4	4	17
8	4	2	2	5	5	1	1	1	1	1	2	1	1	3	4	3	1	2	1	4	2	4	3	2	1	1	5	1	3	5	3	1	2	5	2	2	2	47	18	4	5	7	13	42	11	9	9	13
9	3	3	2	2	4	2	3	2	5	5	5	5	5	5	5	4	5	4	4	3	4	1	1	5	2	2	3	1	1	2	1	5	3	5	2	2	4	80	14	12	20	10	24	40	11	5	8	16
10	4	3	1	4	2	2	2	5	2	1	4	2	2	3	3	1	1	1	1	1	1	3	3	3	2	5	5	5	3	3	5	5	4	4	3	3	5	46	14	11	9	6	6	61	16	13	13	19
11	2	2	3	3	1	1	1	3	1	2	2	2	2	2	1	1	2	3	3	2	3	3	2	1	1	2	1	1	5	5	5	3	1	1	1	4	1	42	11	6	8	3	14	37	9	7	13	8
12	1	4	5	3	3	4	3	5	4	3	5	5	5	5	1	5	5	5	5	4	2	5	3	3	4	4	3	3	5	5	5	4	4	3	3	2	5	82	16	16	18	6	26	61	19	11	14	17
13	3	2	3	2	3	2	1	4	1	1	4	1	4	5	1	2	1	1	2	3	2	1	1	1	3	2	2	1	4	5	2	1	2	4	4	2	1	48	13	8	10	6	11	36	8	7	8	13
14	5	3	5	3	3	2	5	3	4	5	4	5	2	3	5	3	5	4	4	5	4	3	3	3	2	5	3	1	2	2	1	1	3	5	4	3	4	82	19	14	16	8	25	45	16	6	4	19
15	5	1	1	1	1	1	2	1	1	1	2	1	3	2	2	1	1	1	4	1	1	2	1	1	2	1	2	1	3	3	2	2	4	1	4	2	3	34	9	5	7	4	9	34	7	6	7	14
16	3	4	1	1	2	3	1	1	2	2	5	1	4	1	1	1	3	2	5	4	1	4	3	1	4	3	3	5	3	1	5	2	3	3	2	2	3	48	11	7	12	2	16	47	15	11	8	13
17	3	2	5	2	5	4	5	5	3	3	4	3	5	5	4	5	5	3	5	3	3	2	2	4	2	4	1	4	2	1	1	4	4	1	3	2	2	82	17	17	15	9	24	39	14	7	6	12
18	3	2	2	3	1	2	3	3	2	2	1	2	1	2	2	1	2	3	4	2	5	2	5	5	1	1	3	5	1	1	1	1	2	1	3	2	4	48	11	10	6	4	17	38	14	9	3	12
19	4	4	1	1	2	1	1	1	3	1	3	3	2	2	3	1	2	2	1	1	1	1	5	2	5	1	1	3	4	2	3	1	2	1	1	3	1	40	12	6	9	5	8	36	14	8	6	8
20	4	5	3	2	5	2	1	2	2	1	1	3	1	3	2	2	1	3	3	1	1	1	2	5	3	5	1	1	1	1	5	2	1	1	3	5	1	48	19	7	6	5	11	38	16	3	8	11
21	5	4	2	3	2	3	5	4	5	3	4	4	4	5	4	3	5	5	4	2	5	2	1	1	4	2	3	1	1	1	2	5	5	3	4	2	2	81	16	17	15	9	24	39	10	5	8	16
22	3	5	1	4	3	1	1	4	2	1	1	1	3	1	2	2	1	2	4	1	5	1	3	1	3	2	1	2	4	5	1	2	3	1	3	3	2	48	16	8	6	3	15	37	10	7	8	12
23	5	2	4	3	2	2	5	1	5	5	5	1	5	5	5	3	5	4	5	4	5	4	1	2	1	2	2	2	3	3	2	3	2	1	3	4	3	81	16	13	16	10	26	38	10	7	8	13
24	4	5	5	2	3	1	5	2	4	1	1	1	1	1	2	2	3	1	1	1	2	1	1	4	4	5	5	4	2	1	2	3	1	1	1	1	1	48	19	12	4	3	10	37	15	11	6	5
25	4	1	5	2	1	3	2	1	1	3	4	1	1	4	1	1	2	1	1	1	1	3	2	1	4	4	1	3	3	3	1	1	3	1	2	5	2	41	13	7	9	5	7	39	14	7	5	13
26	4	5	4	1	3	4	3	2	5	5	5	5	5	2	4	4	5	3	5	5	3	5	2	2	1	5	4	3	2	1	4	2	4	2	3	5	1	82	17	14	20	6	25	46	15	9	7	15
27	2	1	1	5	4	4	2	2	2	1	1	4	3	3	1	2	2	3	1	3	1	1	3	2	1	1	2	3	2	1	1	1	3	3	4	4	4	48	13	10	9	4	12	36	8	7	3	18

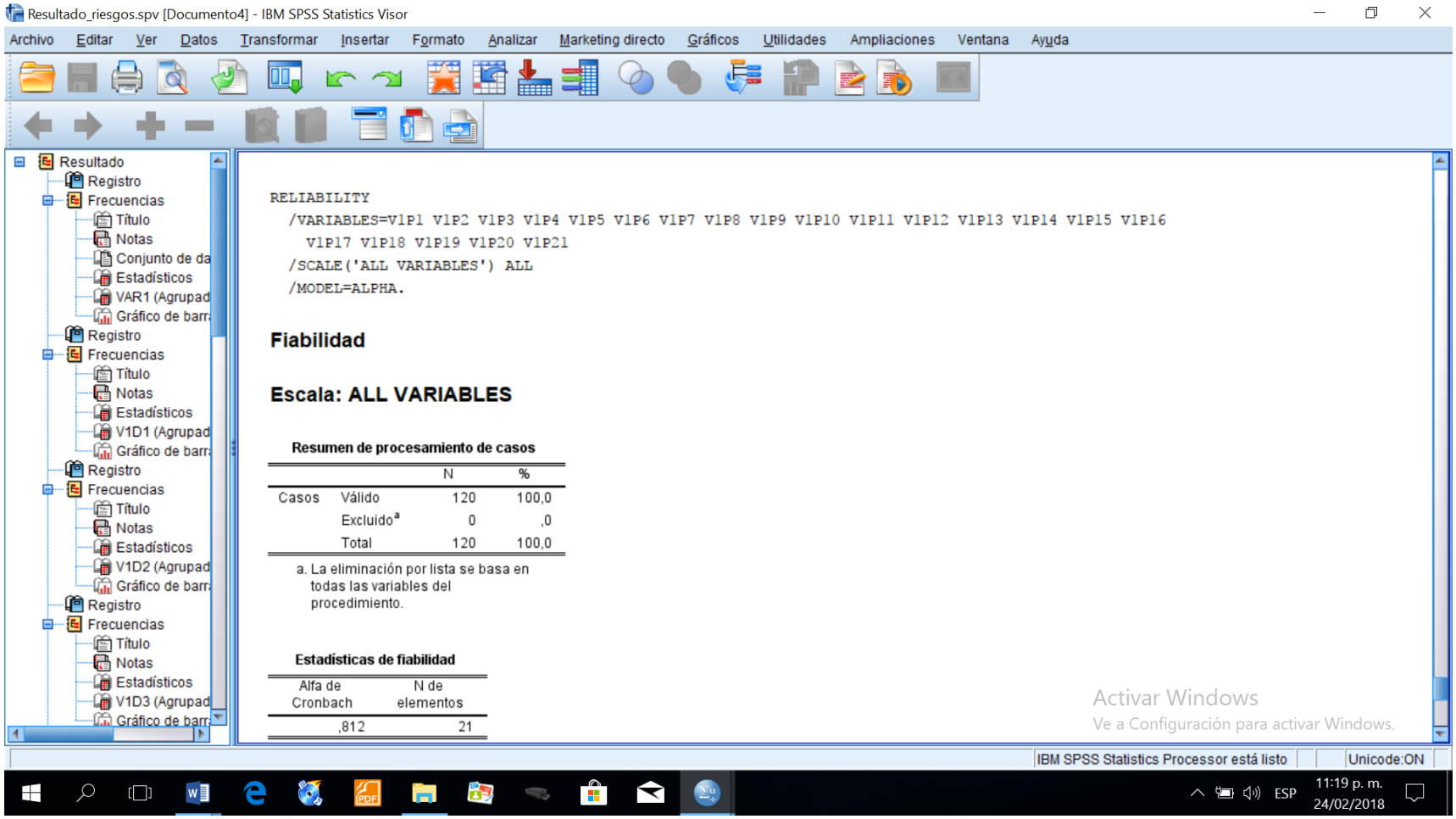
28	3	5	2	1	4	2	2	4	1	3	1	2	1	4	1	4	2	1	1	2	1	5	3	5	2	4	3	4	5	2	5	5	3	5	5	5	2	47	15	9	7	5	11	63	19	12	12	20
29	3	5	4	5	1	4	5	5	5	3	5	5	5	4	3	5	3	5	5	4	3	1	2	2	1	1	2	4	2	4	2	2	1	1	3	1	1	87	18	19	18	7	25	30	7	8	8	7
30	2	3	3	4	1	4	3	1	1	2	3	1	2	2	2	1	3	1	2	4	1	1	2	2	3	1	1	3	1	4	4	1	1	4	3	2	2	46	13	9	8	4	12	35	9	5	9	12
31	2	4	2	3	4	4	3	3	4	4	3	4	5	5	3	5	2	5	5	5	5	5	3	5	1	5	5	3	4	5	5	5	2	5	2	5	2	80	15	14	16	8	27	62	19	12	15	16
32	3	2	3	3	5	1	1	1	4	1	2	3	1	1	2	2	1	2	1	2	4	2	1	5	1	2	5	1	1	2	2	1	4	3	1	4	1	45	16	7	7	3	12	36	11	7	5	13
33	4	2	4	2	2	4	5	5	4	4	4	5	3	2	5	5	5	5	4	5	3	2	2	5	3	1	2	3	5	5	4	5	4	5	5	5	5	82	14	18	16	7	27	61	13	10	14	24
34	2	1	3	1	5	4	3	1	4	1	1	3	1	1	3	1	1	4	3	1	4	4	3	5	5	5	3	2	3	2	3	5	5	5	3	4	5	48	12	12	6	4	14	62	22	8	10	22
35	1	4	2	4	2	5	3	3	4	3	4	3	2	4	1	5	2	3	2	2	2	1	1	2	3	2	1	3	2	4	4	4	2	1	3	4	1	61	13	15	12	5	16	38	9	6	12	11
36	4	2	2	3	2	5	1	2	2	2	1	2	1	1	1	4	1	1	3	1	4	5	5	5	3	2	5	2	4	3	4	3	5	2	5	3	4	45	13	10	6	2	14	60	20	11	10	19
37	5	4	2	4	2	4	1	2	5	5	4	2	3	1	5	2	3	3	1	2	3	2	2	4	2	4	4	3	3	1	1	2	3	2	2	1	1	63	17	12	14	6	14	37	14	10	4	9
38	4	1	1	4	1	3	3	1	4	1	3	3	1	3	2	1	3	2	1	1	4	4	3	2	1	3	1	1	2	4	1	2	2	3	2	4	1	47	11	11	8	5	12	36	13	4	7	12
39	2	3	5	1	3	1	2	4	5	1	1	3	2	2	1	1	4	3	1	2	1	5	2	4	5	3	4	3	4	5	5	2	5	2	3	5	5	48	14	12	7	3	12	62	19	11	12	20
40	3	4	5	3	4	2	3	5	3	5	1	2	2	3	4	1	1	2	2	1	4	3	5	2	1	3	4	2	1	1	2	1	4	2	1	1	4	60	19	13	10	7	11	37	14	7	4	12
41	3	1	1	1	1	4	4	2	4	1	2	1	4	1	1	1	3	1	5	2	4	3	2	5	4	2	5	5	5	4	4	5	2	1	5	5	3	47	7	14	8	2	16	60	16	15	13	16
42	4	2	2	3	2	1	1	5	1	1	1	2	2	1	1	1	2	3	3	2	1	2	1	1	3	1	3	1	2	3	5	2	2	4	4	1	1	41	13	8	6	2	12	36	8	6	10	12
43	5	2	5	4	4	4	4	1	2	5	5	5	4	3	5	3	4	4	1	5	3	5	4	5	3	1	1	1	1	1	3	1	1	2	1	2	5	78	20	11	19	8	20	37	18	3	5	11
44	1	1	1	2	1	1	2	4	3	1	1	2	2	3	1	3	4	1	4	4	3	4	1	1	1	1	2	3	2	4	3	4	2	1	1	1	4	45	6	10	6	4	19	35	8	7	11	9
45	2	2	5	1	5	3	3	2	4	1	1	3	1	2	3	4	1	1	1	1	1	3	1	2	2	3	1	1	1	3	3	4	1	4	2	2	4	47	15	12	6	5	9	37	11	3	10	13
46	4	1	1	2	5	1	4	3	5	2	2	1	1	1	2	3	1	1	1	1	3	1	4	5	2	3	1	4	2	1	1	1	1	3	1	1	5	45	13	13	6	3	10	36	15	7	3	11
47	2	1	1	1	2	2	4	4	2	2	4	3	5	5	4	4	2	4	1	2	1	2	4	4	2	1	4	3	1	2	1	3	2	3	1	1	1	56	7	12	14	9	14	35	13	8	6	8
48	4	1	1	1	3	3	1	2	1	1	3	1	2	3	4	3	4	1	2	3	3	4	1	1	1	1	3	2	3	4	4	4	1	2	1	4	1	47	10	7	7	7	16	37	8	8	12	9
49	5	1	3	1	3	3	1	1	1	3	1	3	2	4	2	1	3	2	2	3	3	1	5	5	5	1	1	2	1	2	2	1	1	2	3	1	1	48	13	6	9	6	14	34	17	4	5	8
50	4	3	1	1	5	2	5	4	3	4	5	4	4	5	1	5	5	5	5	2	3	2	4	2	1	1	2	5	2	2	3	5	2	3	5	2	2	76	14	14	17	6	25	43	10	9	10	14
51	1	4	3	5	1	4	3	1	3	2	1	2	2	1	2	1	1	1	3	3	1	1	2	1	1	3	1	1	3	4	2	3	3	2	1	4	5	45	14	11	7	3	10	37	8	5	9	15
52	5	3	2	4	2	4	5	3	5	3	4	1	1	3	2	3	4	4	1	3	5	5	2	2	4	1	3	1	2	1	2	4	1	1	1	2	5	67	16	17	9	5	20	37	14	6	7	10
53	5	4	1	5	1	1	3	3	2	1	1	1	3	1	1	4	3	1	1	3	3	2	3	3	1	1	1	3	1	1	4	1	4	1	3	4	3	48	16	9	6	2	15	36	10	5	6	15
54	1	1	1	1	3	3	1	1	1	2	4	1	4	4	3	4	3	2	2	2	1	2	1	1	3	3	5	1	3	5	4	1	3	1	1	1	1	45	7	6	11	7	14	36	10	9	10	7
55	2	1	3	1	4	1	4	4	1	2	3	2	2	1	1	2	3	1	4	1	1	3	5	2	1	5	1	3	3	1	2	2	1	1	2	1	3	44	11	10	9	2	12	36	16	7	5	8
56	5	2	1	4	1	4	3	1	2	2	1	1	1	2	1	1	1	1	3	1	3	5	2	3	1	1	2	1	4	3	1	1	3	3	2	1	3	41	13	10	5	3	10	36	12	7	5	12
57	1	1	2	1	1	2	1	2	1	1	3	2	3	1	2	1	2	1	1	1	2	5	4	3	5	5	4	4	4	2	4	4	5	3	4	5	1	32	6	6	9	3	8	62	22	12	10	18
58	4	5	2	5	5	3	1	1	4	1	1	2	1	1	1	1	1	1	2	1	1	4	5	2	5	1	2	2	3	1	1	2	1	1	1	3	2	44	21	9	5	2	7	36	17	7	4	8
59	4	2	2	1	1	5	1	5	3	3	2	4	1	2	1	4	2	4	4	4	3	2	2	1	2	1	1	1	2	4	4	3	1	4	1	3	4	58	10	14	10	3	21	36	8	4	11	13
60	2	1	3	1	1	4	1	3	1	1	2	2	3	1	1	2	3	4	3	1	5	3	5	4	2	5	3	1	5	3	1	4	3	5	1	2	4	45	8	9	8	2	18	51	19	9	8	15
61	4	3	4	2	3	1	5	1	2	4	2	5	1	4	2	2	1	5	1	1	3	1	5	1	3	4	1	1	3	1	4	2	4	1	1	3	1	56	16	9	12	6	13	36	14	5	7	10
62	5	3	1	2	3	1	5	1	3	1	2	4	2	1	1	3	1	1	3	3	1	1	5	2	3	1	1	2	5	5	1	3	2	2	1	1	2	47	14	10	9	2	12	37	12	8	9	8
63	2	4	3	2	1	2	2	5	2	5	1	1	4	1	2	5	1	2	5	1	5	2	4	4	3	3	4	4	2	1	1	3	2	4	4	1	5	56	12	11	11	3	19	47	16	10	5	16
64	3	2	1	1	1	1	1	5	1	1	2	3	1	1	2	3	3	2	1	1	1	5	5	5	5	1	5	5	3	5	1	5	5	1	3	5	5	37	8	8	7	3	11	64	21	13	11	19
65	2	2	5	5	3	1	3	1	4	4	4	1	4	4	1	2	2	2	1	4	3	2	2	3	5	1	5	4	4	4	4	5	2	4	3	4	3	58	17	9	13	5	14	55	13	13	13	16
66	1	3	1	1	1	3	2	4	3	1	4	2	3	1	1	4	1	3	1	1	4	4	1	1	1	1	2	2	5	2	1	1	3	2	1	4	2	45	7	12	10	2	14	33	8	9	4	12

67	3	3	5	4	3	5	1	2	5	1	1	1	1	1	1	2	2	2	2	1	1	1	1	1	2	2	4	1	2	5	2	4	4	2	1	3	1	47	18	13	4	2	10	36	7	7	11	11
68	5	4	2	4	3	4	5	4	4	3	4	4	1	5	5	1	2	5	2	1	5	4	4	2	1	3	1	2	1	1	4	4	3	3	3	2	4	73	18	17	12	10	16	42	14	4	9	15
69	1	1	1	2	2	1	4	1	1	2	1	3	1	2	3	1	2	1	2	2	1	1	5	5	5	5	1	3	5	4	5	1	4	4	5	5	5	35	7	7	7	5	9	63	21	9	10	23
70	2	4	1	1	4	2	5	3	2	1	2	3	5	2	1	2	5	2	2	5	1	3	5	4	2	1	1	2	1	3	3	1	3	2	1	1	3	55	12	12	11	3	17	36	15	4	7	10
71	2	5	5	2	4	2	4	1	1	2	1	1	3	1	1	1	1	3	1	3	3	1	4	1	5	3	4	1	2	1	1	3	2	2	1	4	1	47	18	8	7	2	12	36	14	7	5	10
72	5	1	5	1	3	4	2	5	2	5	4	1	4	5	5	4	2	1	5	1	2	4	2	1	1	1	2	2	4	1	2	1	1	4	1	1	5	67	15	13	14	10	15	33	9	8	4	12
73	4	4	2	4	1	3	5	1	1	1	2	1	3	1	1	2	1	4	2	3	1	4	5	5	5	4	3	4	2	2	1	3	2	1	5	3	2	47	15	10	7	2	13	51	23	9	6	13
74	2	2	5	5	1	2	1	2	1	5	5	5	3	4	2	5	2	1	2	5	4	1	1	5	3	3	3	1	2	2	4	1	1	1	2	4	1	64	15	6	18	6	19	35	13	6	7	9
75	4	1	4	1	3	3	3	1	3	1	1	1	2	1	3	3	3	2	2	3	1	2	3	2	3	2	4	2	1	2	3	4	4	1	3	2	2	46	13	10	5	4	14	40	12	7	9	12
76	3	4	2	5	2	3	2	1	3	5	4	4	3	2	2	2	2	3	1	3	1	4	2	1	1	5	2	2	4	5	4	1	1	1	4	2	4	57	16	9	16	4	12	43	13	8	10	12
77	5	3	2	3	1	1	4	3	3	1	2	1	4	1	3	2	1	1	1	2	2	2	2	1	1	3	3	2	1	2	1	5	3	1	3	1	4	46	14	11	8	4	9	35	9	6	8	12
78	3	2	5	1	3	5	2	4	2	3	3	2	1	2	2	1	4	3	1	1	3	4	3	5	1	4	5	4	4	5	3	1	5	1	2	1	1	53	14	13	9	4	13	49	17	13	9	10
79	4	3	1	2	2	1	3	1	3	3	2	1	4	5	1	2	2	3	1	3	1	5	1	2	1	2	2	1	1	3	5	2	1	1	1	4	1	48	12	8	10	6	12	33	11	4	10	8
80	2	4	2	5	4	2	2	1	5	1	1	5	5	5	2	5	4	3	1	1	2	3	4	2	5	1	2	5	2	4	5	5	1	4	4	5	5	62	17	10	12	7	16	57	15	9	14	19
81	1	3	1	1	3	3	1	3	2	1	1	1	3	2	2	2	1	1	3	3	4	5	5	4	1	2	5	5	3	1	5	5	5	5	5	5	5	42	9	9	6	4	14	66	17	13	11	25
82	5	1	1	1	3	3	1	1	2	2	2	3	5	3	1	3	3	1	3	1	1	5	1	4	4	1	1	1	4	1	3	2	3	2	1	1	3	46	11	7	12	4	12	37	15	6	6	10
83	1	3	2	3	5	2	3	5	1	5	4	2	2	4	4	2	2	1	4	3	3	4	1	1	3	1	3	1	1	1	1	4	3	1	4	2	2	61	14	11	13	8	15	33	10	5	6	12
84	4	2	1	1	1	3	1	2	1	2	1	1	2	3	5	1	1	4	2	3	2	3	1	1	1	2	3	1	1	4	3	4	1	1	2	3	5	43	9	7	6	8	13	36	8	5	11	12
85	4	2	4	1	3	2	1	5	1	1	2	4	4	4	4	3	1	5	3	2	5	2	3	3	4	2	3	2	5	4	2	4	2	2	5	4	2	61	14	9	11	8	19	49	14	10	10	15
86	2	1	1	1	2	1	1	1	3	4	1	2	3	2	1	4	5	3	4	4	1	2	5	4	3	2	2	5	2	3	3	5	5	5	4	1	5	47	7	6	10	3	21	56	16	9	11	20
87	2	3	5	3	1	2	1	4	2	3	4	3	1	2	1	1	3	1	1	1	1	1	2	2	3	4	5	2	4	2	1	1	1	2	2	3	1	45	14	9	11	3	8	36	12	11	4	9
88	3	1	1	1	3	1	5	4	1	1	4	3	1	5	1	5	3	2	5	1	1	4	2	2	2	4	5	5	1	3	3	2	1	3	4	2	3	52	9	11	9	6	17	46	14	11	8	13
89	5	2	1	1	3	1	1	4	1	2	4	5	1	1	1	1	4	4	2	2	1	1	1	5	1	1	1	3	1	4	3	1	3	5	1	1	4	47	12	7	12	2	14	36	9	5	8	14
90	4	4	2	3	5	4	1	3	3	5	5	4	2	5	5	4	2	2	4	1	2	2	1	5	3	3	4	4	1	4	5	1	1	5	2	2	2	70	18	11	16	10	15	45	14	9	10	12
91	3	2	3	5	4	1	1	3	1	1	2	1	4	1	4	1	2	3	1	1	1	4	5	2	4	1	5	3	2	1	1	5	4	2	2	4	1	45	17	6	8	5	9	46	16	10	7	13
92	1	4	3	3	2	1	2	3	1	3	4	4	3	3	2	4	4	1	2	2	2	3	2	2	4	2	3	1	2	1	5	1	2	2	1	1	1	54	13	7	14	5	15	33	13	6	7	7
93	5	3	3	1	1	2	1	3	3	2	1	3	1	2	3	3	1	1	2	3	2	1	3	4	2	1	2	1	5	5	5	2	5	2	3	5	5	46	13	9	7	5	12	51	11	8	12	20
94	1	2	1	4	5	3	3	3	2	2	4	5	4	5	1	3	5	3	3	1	1	2	2	2	1	1	3	2	1	1	2	4	2	2	4	4	3	61	13	11	15	6	16	36	8	6	7	15
95	1	1	2	3	1	3	1	1	2	2	1	1	1	3	1	1	2	1	3	2	3	1	3	1	2	1	4	5	2	3	3	4	5	5	5	4	1	36	8	7	5	4	12	49	8	11	10	20
96	4	4	2	4	4	5	3	1	4	5	5	4	1	5	2	5	5	4	1	1	4	2	3	1	1	1	4	1	1	3	3	1	2	5	1	3	4	73	18	13	15	7	20	36	8	6	7	15
97	4	3	1	4	1	1	1	1	3	1	2	1	4	1	4	1	4	1	2	1	1	4	1	5	5	5	5	5	3	1	1	5	5	5	3	2	3	42	13	6	8	5	10	58	20	13	7	18
98	5	1	5	1	1	2	5	2	5	4	2	4	5	3	3	5	3	2	5	2	5	5	5	2	3	5	5	2	4	4	4	1	1	5	5	5	4	70	13	14	15	6	22	60	20	11	9	20
99	2	3	2	5	5	3	1	4	1	1	2	2	4	1	3	1	1	1	2	1	1	3	1	1	5	1	1	3	1	1	3	2	3	2	4	4	1	46	17	9	9	4	7	36	11	5	6	14
100	1	1	2	1	1	1	1	3	1	3	1	3	2	1	1	2	4	2	4	1	3	4	5	1	2	3	5	2	5	4	2	5	4	5	3	1	5	39	6	6	9	2	16	56	15	12	11	18
101	1	3	1	1	4	3	5	3	4	5	1	3	1	1	2	2	1	3	1	4	1	4	1	3	1	1	2	1	5	2	1	2	1	2	1	2	2	50	10	15	10	3	12	31	10	8	5	8
102	1	3	2	2	3	3	5	1	2	4	1	1	3	1	2	1	2	1	2	3	1	3	4	5	5	4	5	4	4	5	3	3	3	4	5	3	1	44	11	11	9	3	10	61	21	13	11	16

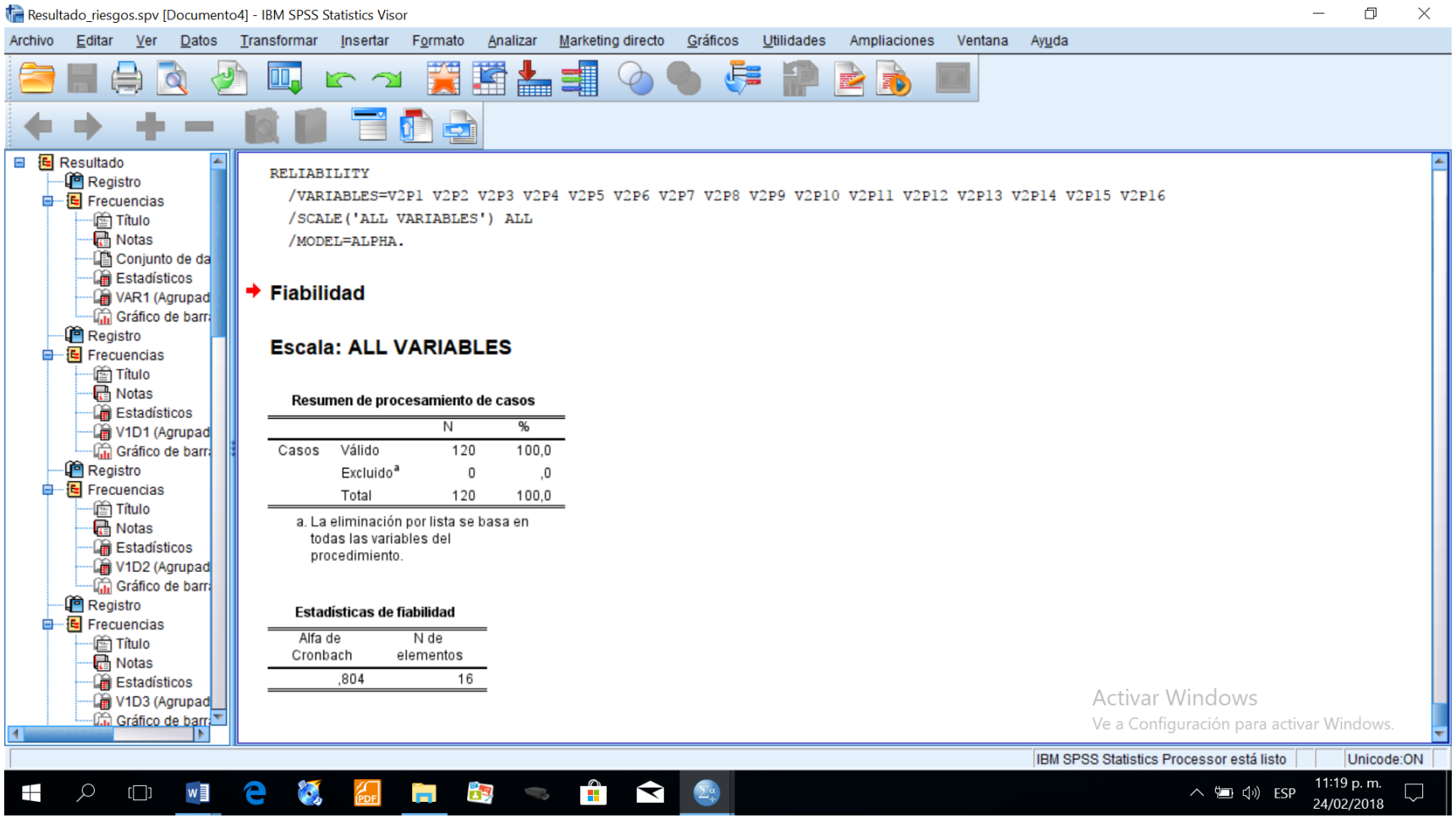
103	4	5	5	1	4	1	1	4	4	4	2	2	2	3	3	3	5	4	5	5	3	2	4	1	4	5	5	2	3	2	5	1	5	4	4	4	4	70	19	10	10	6	25	55	16	10	8	21
104	3	2	5	1	1	1	4	1	2	2	1	3	2	2	3	2	3	2	1	2	1	1	2	2	3	3	1	3	3	2	1	1	3	1	1	1	3	44	12	8	8	5	11	31	11	7	4	9
105	1	2	2	5	2	4	3	3	4	3	2	4	1	2	5	3	4	4	4	3	3	1	4	1	2	1	1	1	2	2	5	4	1	1	1	1	4	64	12	14	10	7	21	32	9	4	11	8
106	2	1	2	1	1	2	1	2	3	4	1	1	4	2	3	5	2	1	4	2	2	5	1	4	2	2	5	2	4	3	5	2	3	5	4	4	4	46	7	8	10	5	16	55	14	11	10	20
107	4	3	1	2	2	4	2	2	1	2	1	5	4	2	2	5	4	3	2	3	2	5	4	2	3	5	4	2	5	5	1	3	1	5	5	5	5	56	12	9	12	4	19	60	19	11	9	21
108	3	1	1	3	2	1	1	3	4	3	1	3	2	2	1	1	4	1	3	1	5	1	1	4	4	1	1	4	2	2	1	1	1	1	2	2	3	46	10	9	9	3	15	31	11	7	4	9
109	1	2	1	3	1	1	3	1	1	1	1	2	2	1	3	4	4	3	5	3	3	2	4	2	2	2	1	5	3	3	2	5	5	3	1	3	4	46	8	6	6	4	22	47	12	9	10	16
110	3	4	3	2	1	1	4	4	2	1	2	2	3	1	1	1	2	1	1	2	1	4	1	2	4	3	2	1	1	5	2	1	4	3	3	3	1	42	13	11	8	2	8	40	14	4	8	14
111	3	5	4	2	2	4	5	2	1	3	4	5	4	3	5	4	4	5	3	1	3	3	1	2	2	1	1	2	1	2	1	3	2	1	3	1	3	72	16	12	16	8	20	29	9	4	6	10
112	3	4	1	1	1	1	3	2	4	1	3	1	2	4	1	2	1	2	1	3	4	4	1	3	3	2	2	1	2	4	1	1	3	1	3	1	5	45	10	10	7	5	13	37	13	5	6	13
113	1	4	5	3	3	1	5	5	4	5	5	5	4	5	1	3	3	5	1	1	2	3	5	1	5	3	1	1	2	2	1	4	2	5	5	5	1	71	16	15	19	6	15	46	17	4	7	18
114	2	4	4	1	1	1	1	1	1	2	1	1	1	1	1	4	5	3	4	3	1	5	2	5	1	1	1	4	1	1	2	2	2	3	3	1	1	43	12	4	5	2	20	35	14	6	5	10
115	2	2	3	4	1	1	1	3	4	1	1	1	3	3	1	1	3	1	2	1	4	2	5	3	4	4	4	3	5	4	4	4	2	4	5	4	5	43	12	9	6	4	12	62	18	12	12	20
116	3	5	3	1	1	2	3	1	1	3	1	1	2	1	4	1	4	2	1	3	5	3	1	1	3	1	2	3	1	1	4	3	1	2	2	1	1	48	13	7	7	5	16	30	9	6	8	7
117	2	2	1	1	3	1	1	1	3	2	2	1	3	5	2	2	3	2	2	1	2	3	1	3	1	1	4	1	1	1	1	3	3	2	5	4	1	42	9	6	8	7	12	35	9	6	5	15
118	3	2	3	2	2	3	3	1	3	2	2	1	1	2	4	2	1	1	3	2	3	5	5	2	2	4	5	5	1	5	1	3	5	4	5	5	3	46	12	10	6	6	12	60	18	11	9	22
119	1	4	4	1	3	2	2	2	3	3	3	2	1	3	2	3	1	2	1	1	1	1	2	1	1	2	2	5	2	1	1	2	1	3	2	2	4	45	13	9	9	5	9	32	7	9	4	12
120	4	3	2	3	5	2	2	4	1	1	1	2	4	2	5	3	5	3	3	3	4	5	3	5	5	2	5	4	5	5	2	1	4	4	2	5	5	62	17	9	8	7	21	62	20	14	8	20

Anexo5: Tablas y gráficos alternos del capítulo resultados

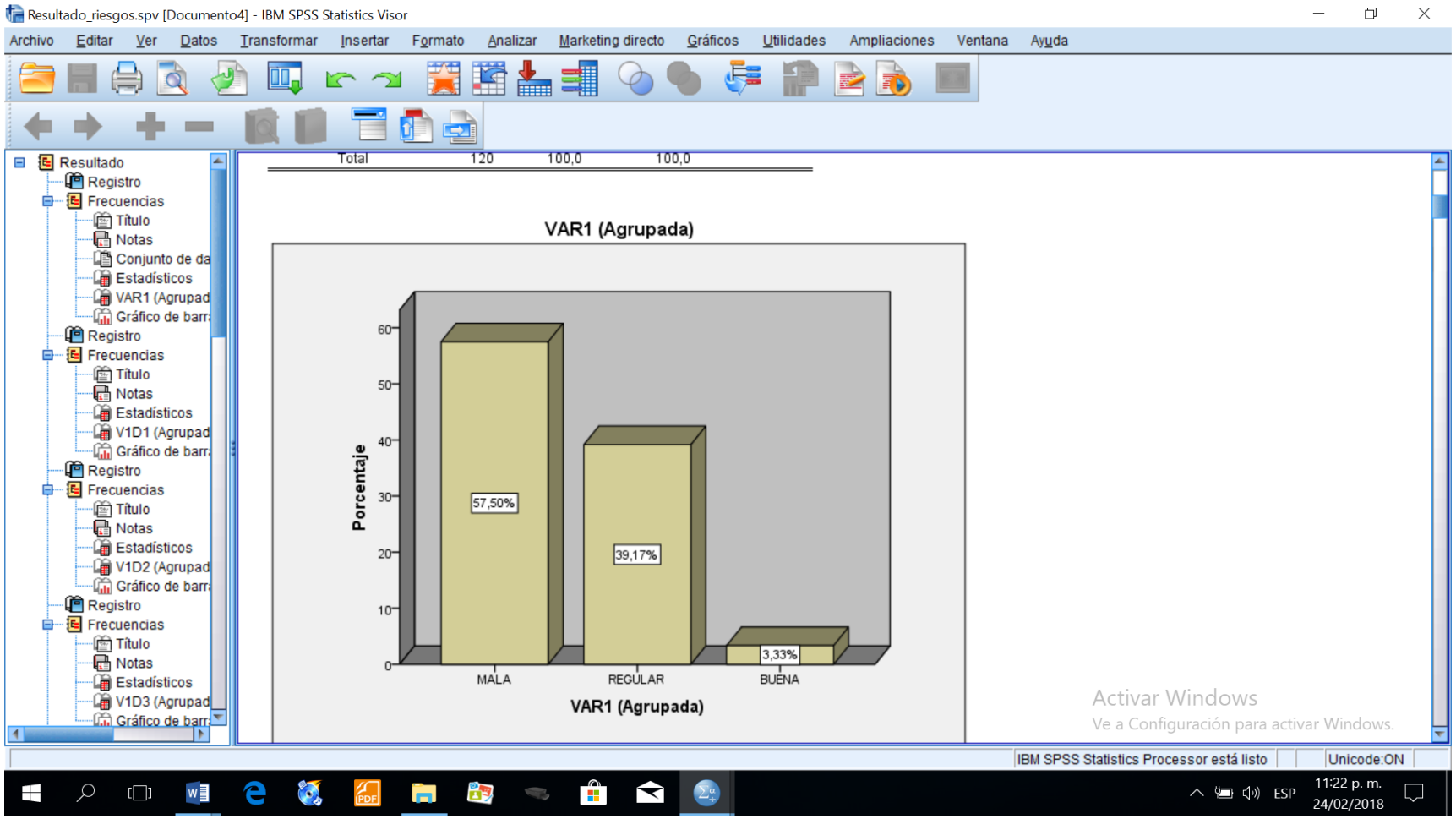
Análisis de fiabilidad variable gestión de riesgos:



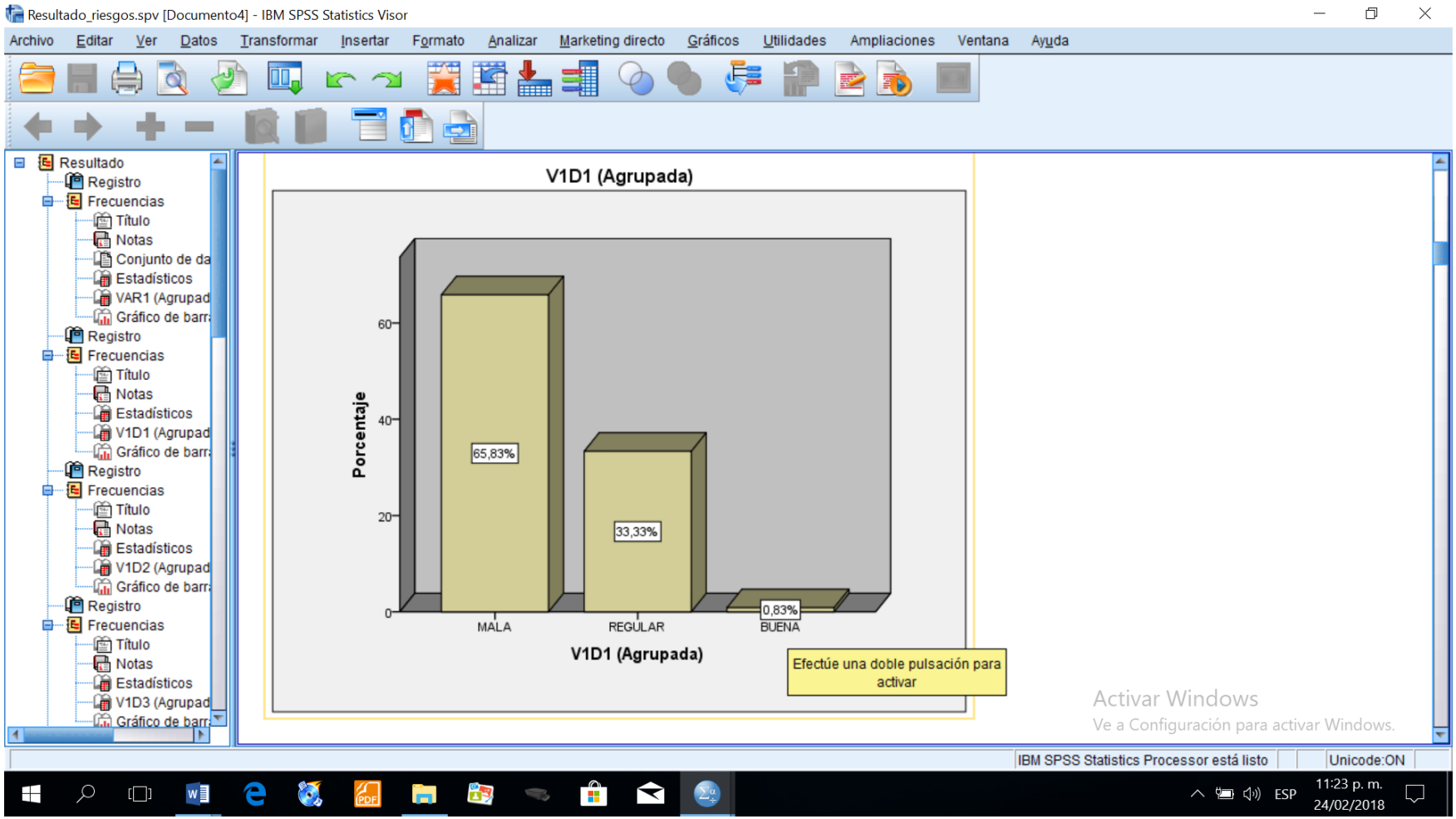
Análisis de fiabilidad variable seguridad de la información:



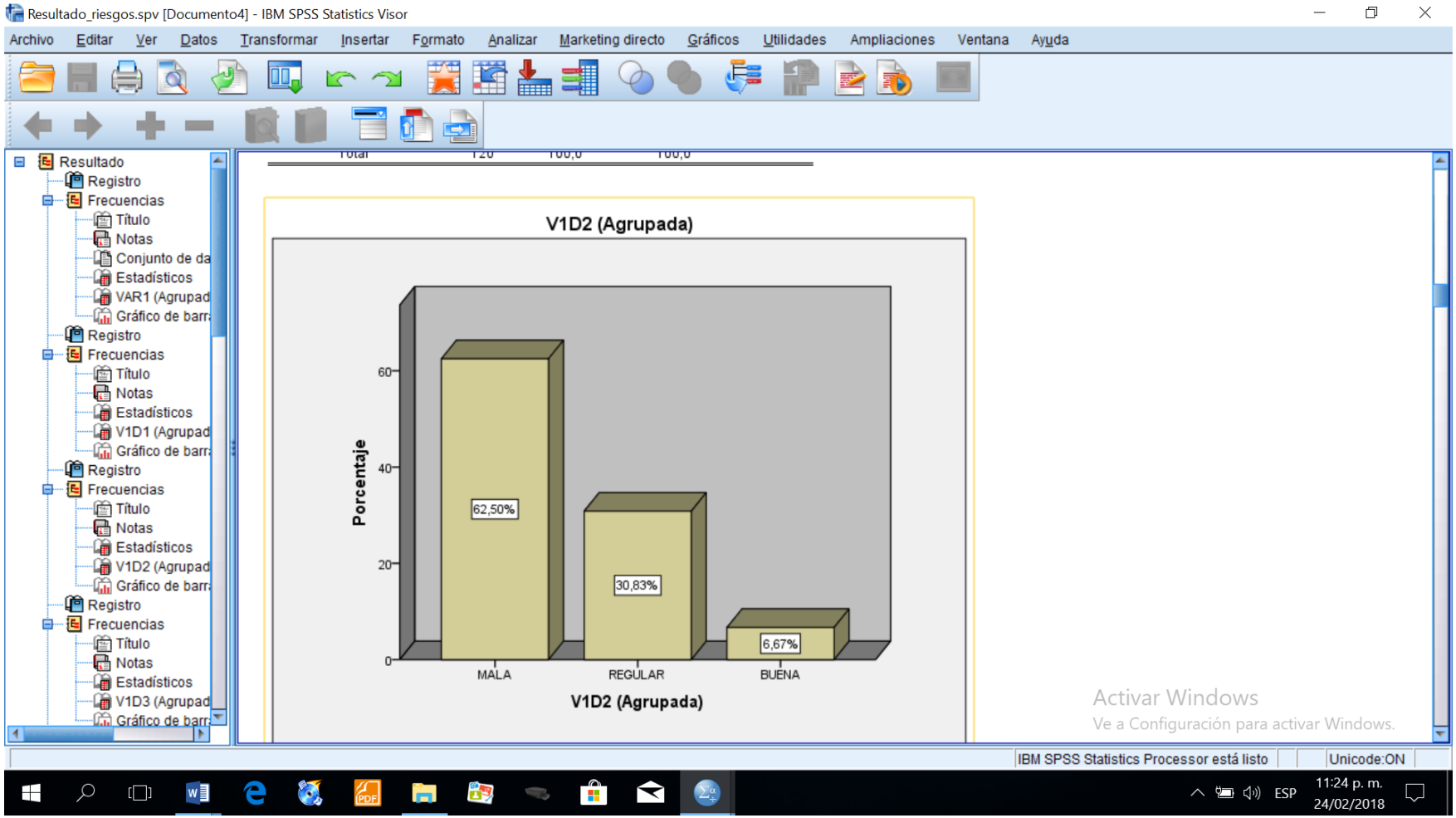
Análisis descriptivo de frecuencias variable gestión de riesgos:



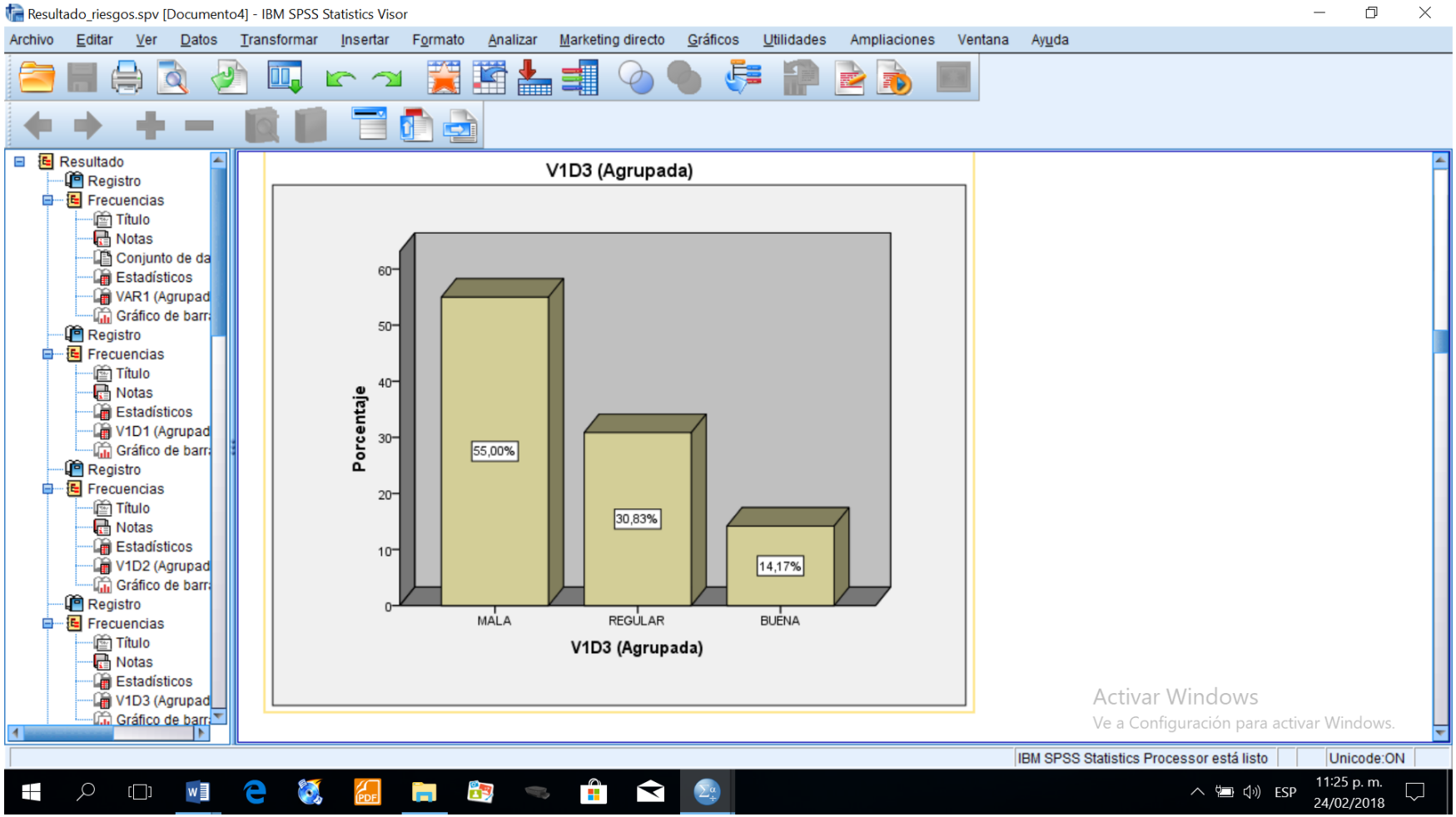
Análisis descriptivos de frecuencias de la dimensión activos de información de la variable gestión de riesgos:



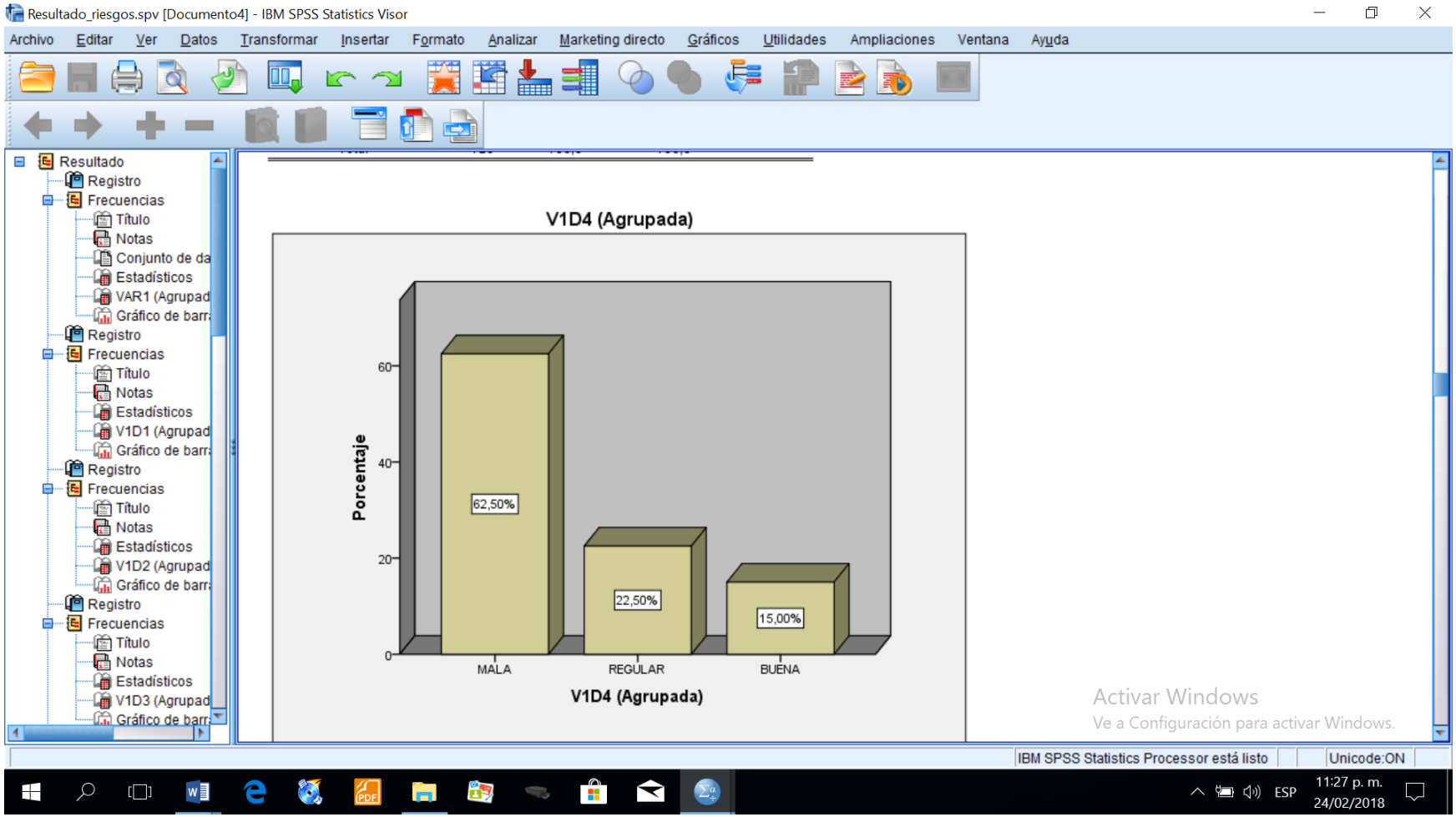
Análisis descriptivo de frecuencias de la dimensión amenazas de la variable gestión de riesgos:



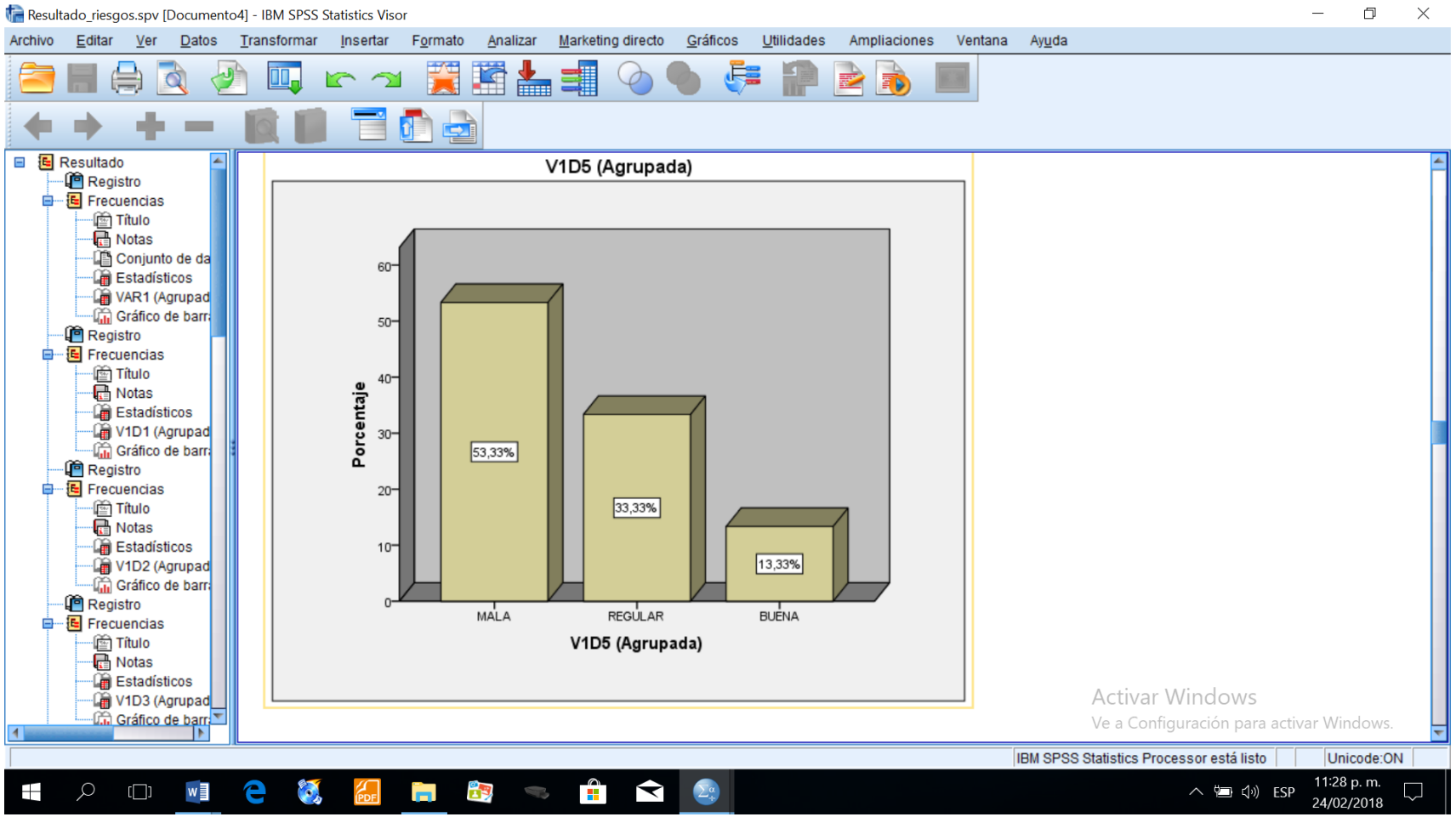
Análisis descriptivo de frecuencias de la dimensión impacto potencial de la variable gestión de riesgos:



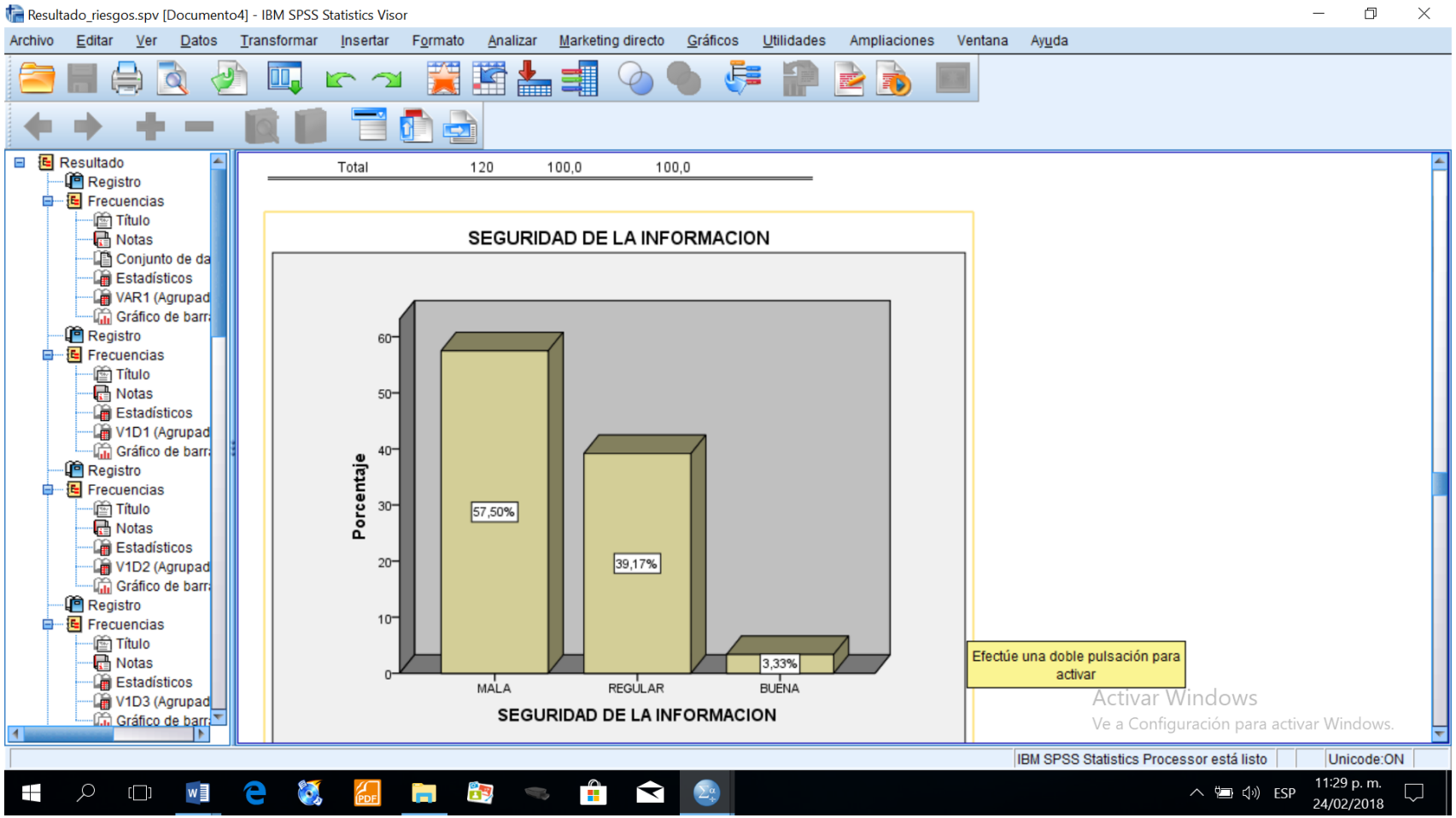
Análisis descriptivo de frecuencias de la dimensión Riesgo potencial de la variable gestión de riesgos:



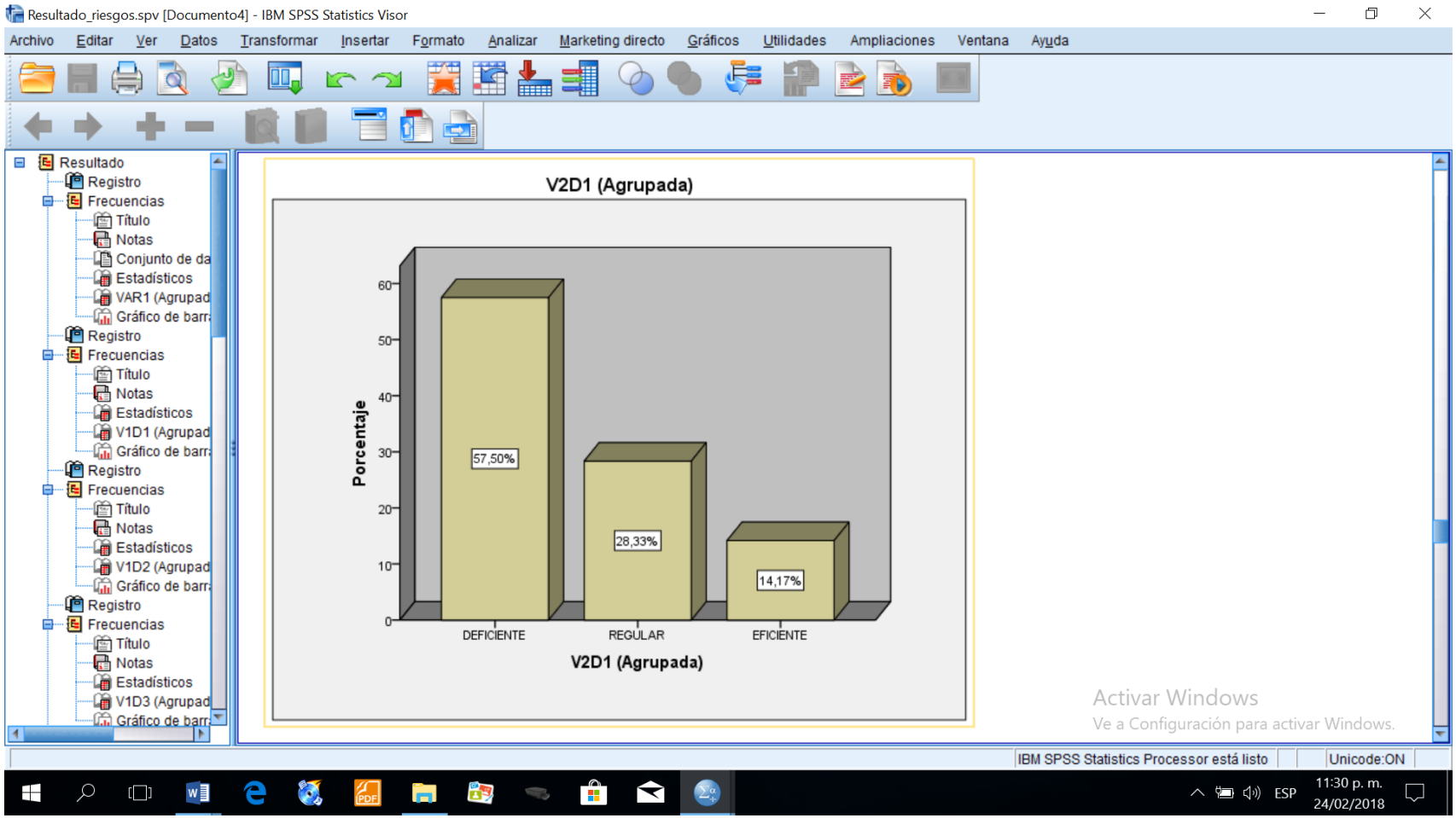
Análisis descriptivo de frecuencias de la dimensión Salvaguardas de la variable gestión de riesgos:



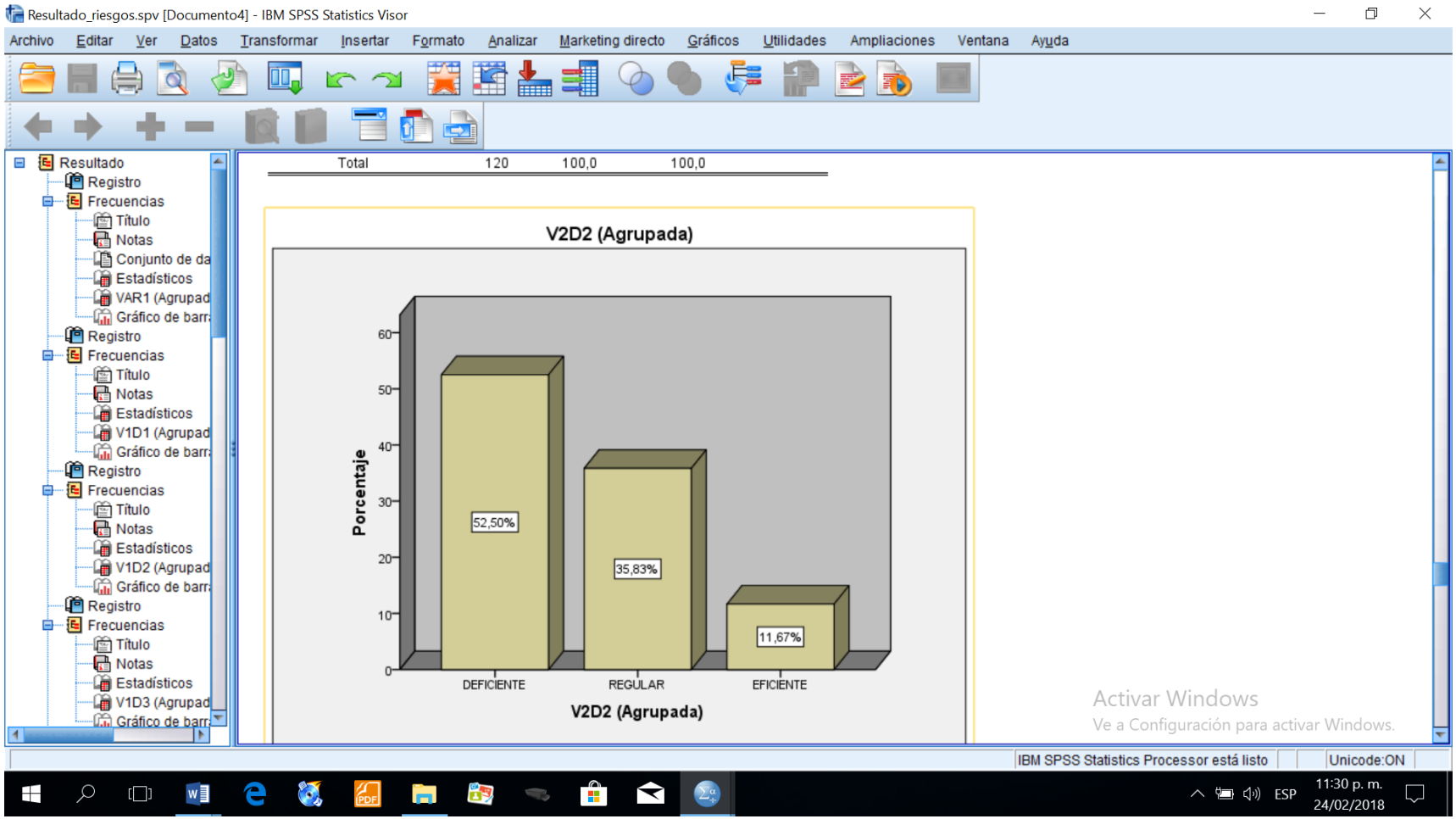
Análisis descriptivo de frecuencias de la variable seguridad de la información:



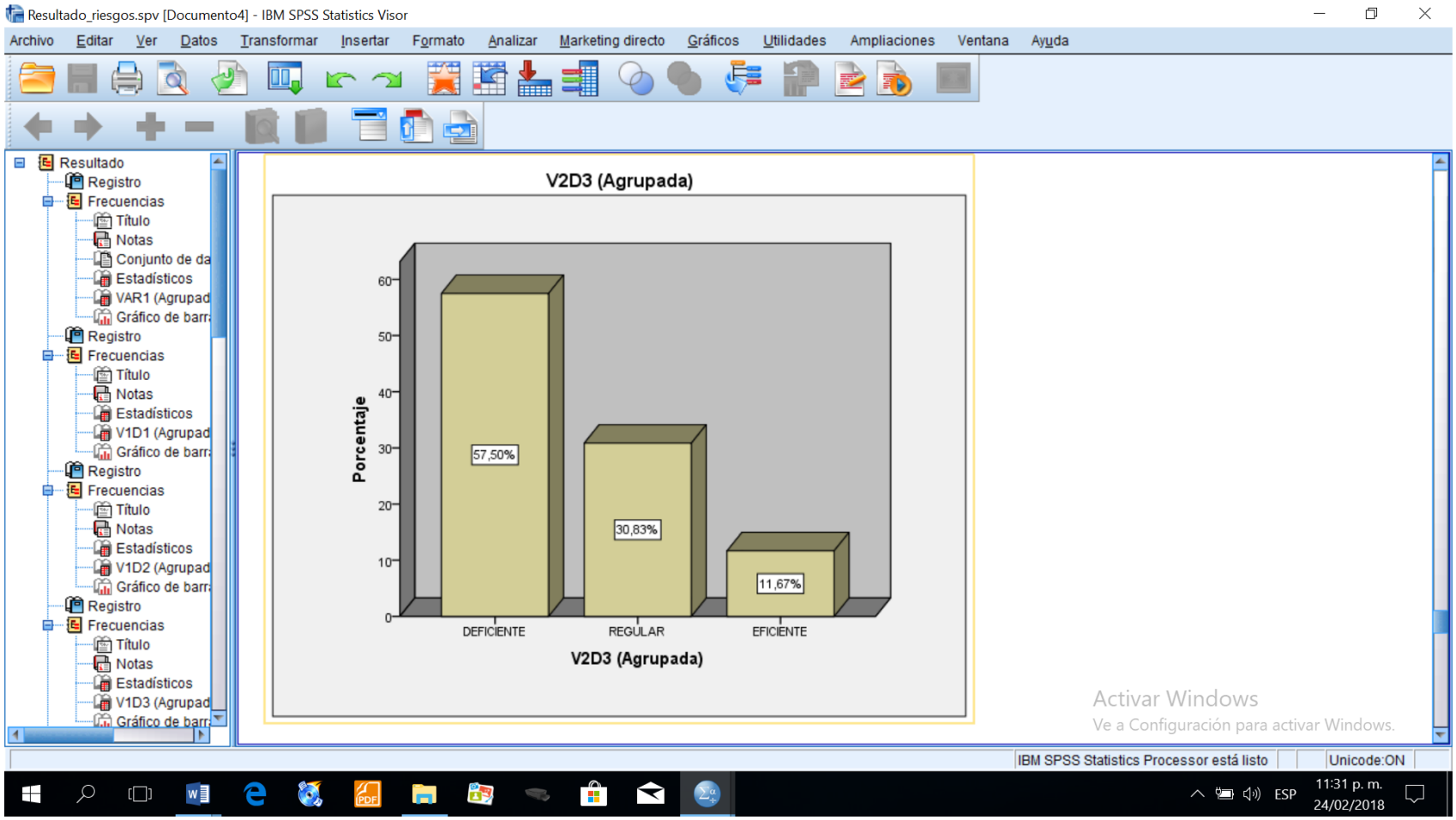
Análisis descriptivo de frecuencias de la dimensión técnico de la variable seguridad de la información:



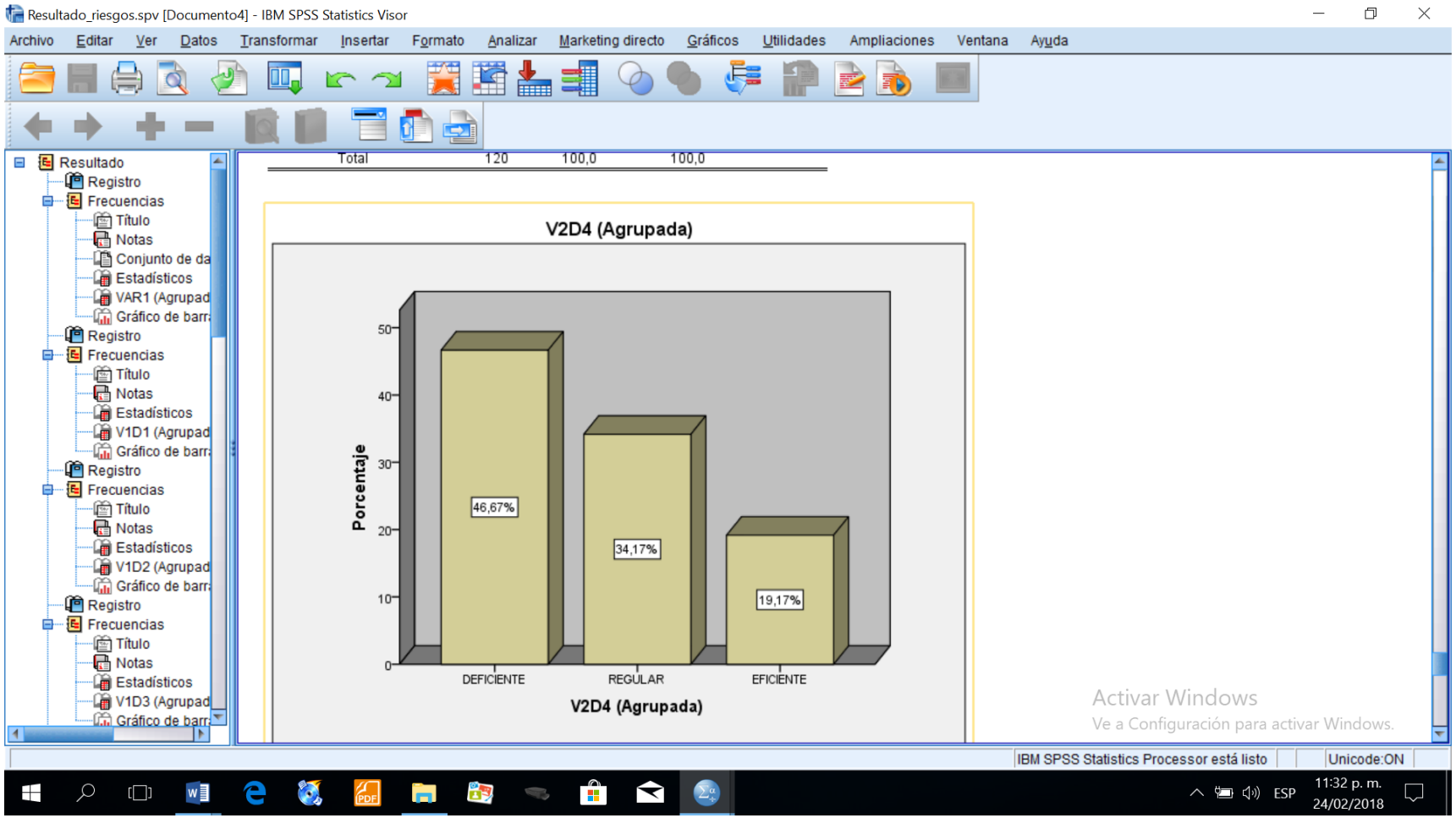
Análisis descriptivo de frecuencias de la dimensión legal de la variable seguridad de la información:



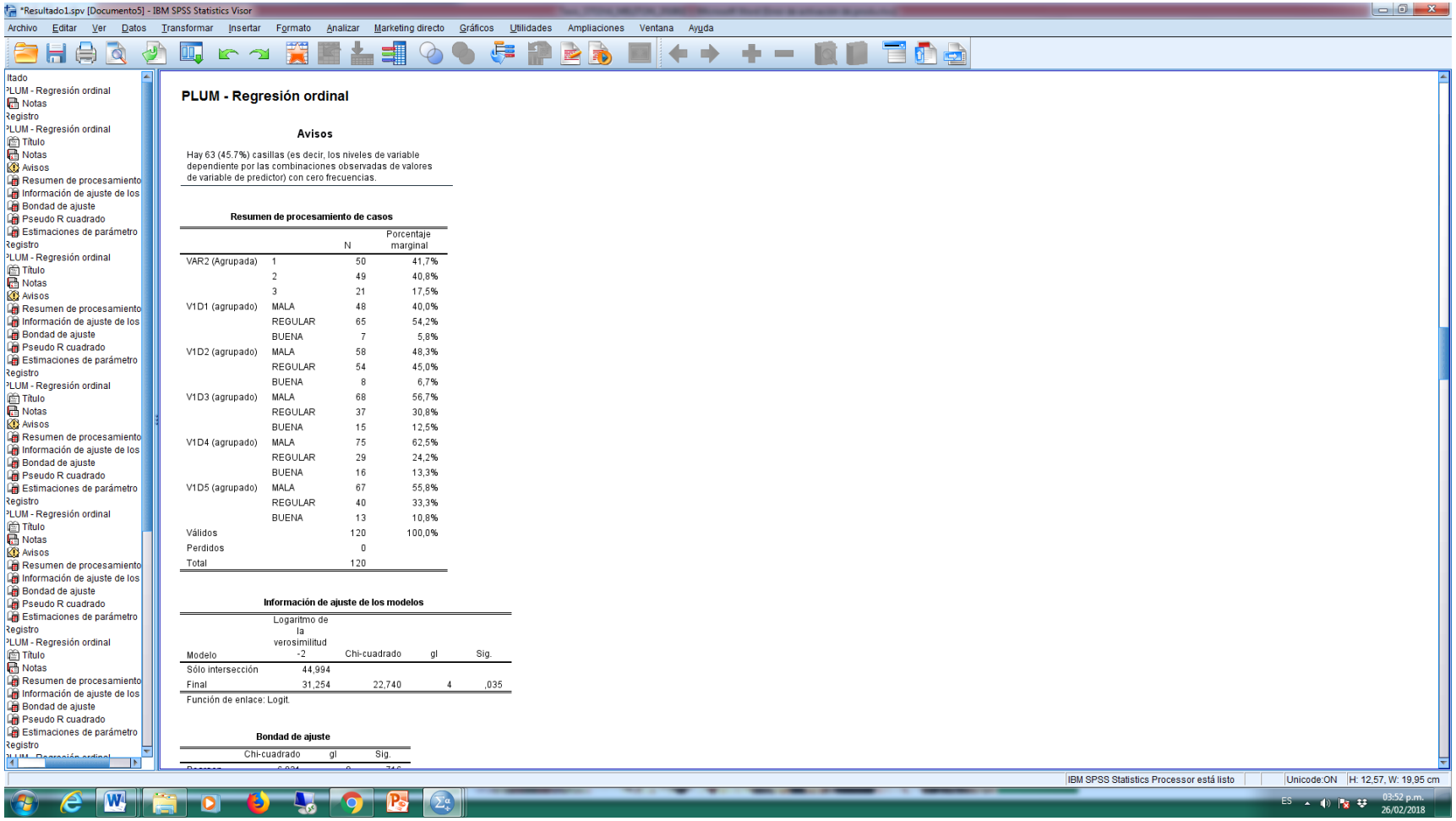
Análisis descriptivo de frecuencias de la dimensión humano de la variable seguridad de la información:



Análisis descriptivo de frecuencias de la dimensión organizativo de la variable seguridad de la información:



Ajuste de datos para el modelo de gestión de riesgos de TI en la seguridad de la información de Agrorural.



Resumen de procesamiento de casos

		N	Porcentaje marginal
VAR2 (Agrupada)	1	50	41,7%
	2	49	40,8%
	3	21	17,5%
V1D1 (agrupado)	MALA	48	40,0%
	REGULAR	65	54,2%
	BUENA	7	5,8%
V1D2 (agrupado)	MALA	58	48,3%
	REGULAR	54	45,0%
	BUENA	8	6,7%
V1D3 (agrupado)	MALA	68	56,7%
	REGULAR	37	30,8%
	BUENA	15	12,5%
V1D4 (agrupado)	MALA	75	62,5%
	REGULAR	29	24,2%
	BUENA	16	13,3%
V1D5 (agrupado)	MALA	67	55,8%
	REGULAR	40	33,3%
	BUENA	13	10,8%
Válidos		120	100,0%
Perdidos		0	
Total		120	

Información de ajuste de los modelos

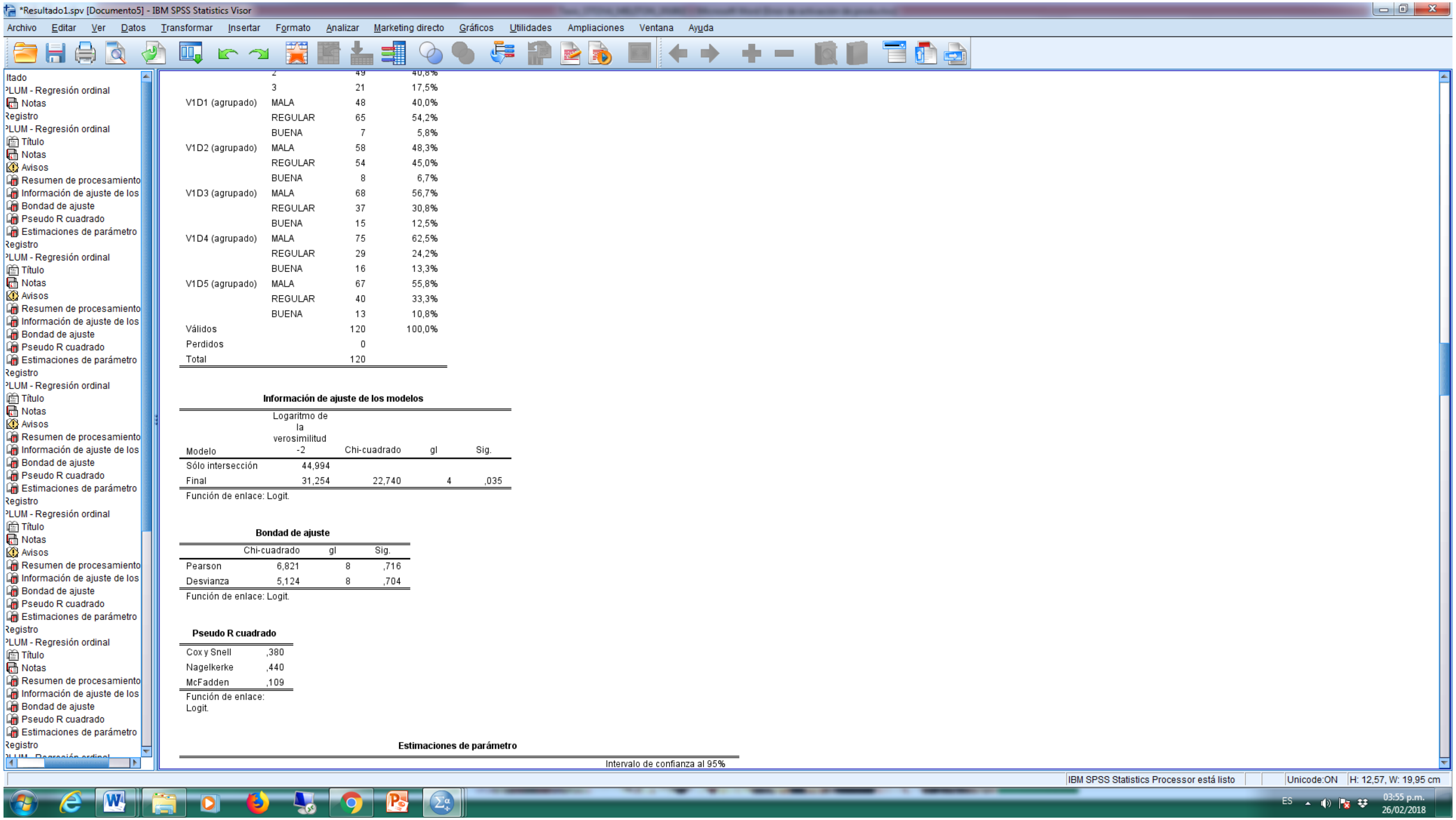
Modelo	Logaritmo de la verosimilitud -2	Chi-cuadrado	gl	Sig.
Sólo intersección	44,994			
Final	31,254	22,740	4	,035

Función de enlace: Logit.

Bondad de ajuste

	Chi-cuadrado	gl	Sig.

Determinación de las variables para el modelo de regresión logística ordinal, bondad de ajustes.



	2	49	40,8%
	3	21	17,5%
V1D1 (agrupado)	MALA	48	40,0%
	REGULAR	65	54,2%
	BUENA	7	5,8%
V1D2 (agrupado)	MALA	58	48,3%
	REGULAR	54	45,0%
	BUENA	8	6,7%
V1D3 (agrupado)	MALA	68	56,7%
	REGULAR	37	30,8%
	BUENA	15	12,5%
V1D4 (agrupado)	MALA	75	62,5%
	REGULAR	29	24,2%
	BUENA	16	13,3%
V1D5 (agrupado)	MALA	67	55,8%
	REGULAR	40	33,3%
	BUENA	13	10,8%
Válidos		120	100,0%
Perdidos		0	
Total		120	

Información de ajuste de los modelos

Modelo	Logaritmo de la verosimilitud -2	Chi-cuadrado	gl	Sig.
Sólo intersección	44,994			
Final	31,254	22,740	4	,035

Función de enlace: Logit.

Bondad de ajuste

	Chi-cuadrado	gl	Sig.
Pearson	6,821	8	,716
Desvianza	5,124	8	,704

Función de enlace: Logit.

Pseudo R cuadrado

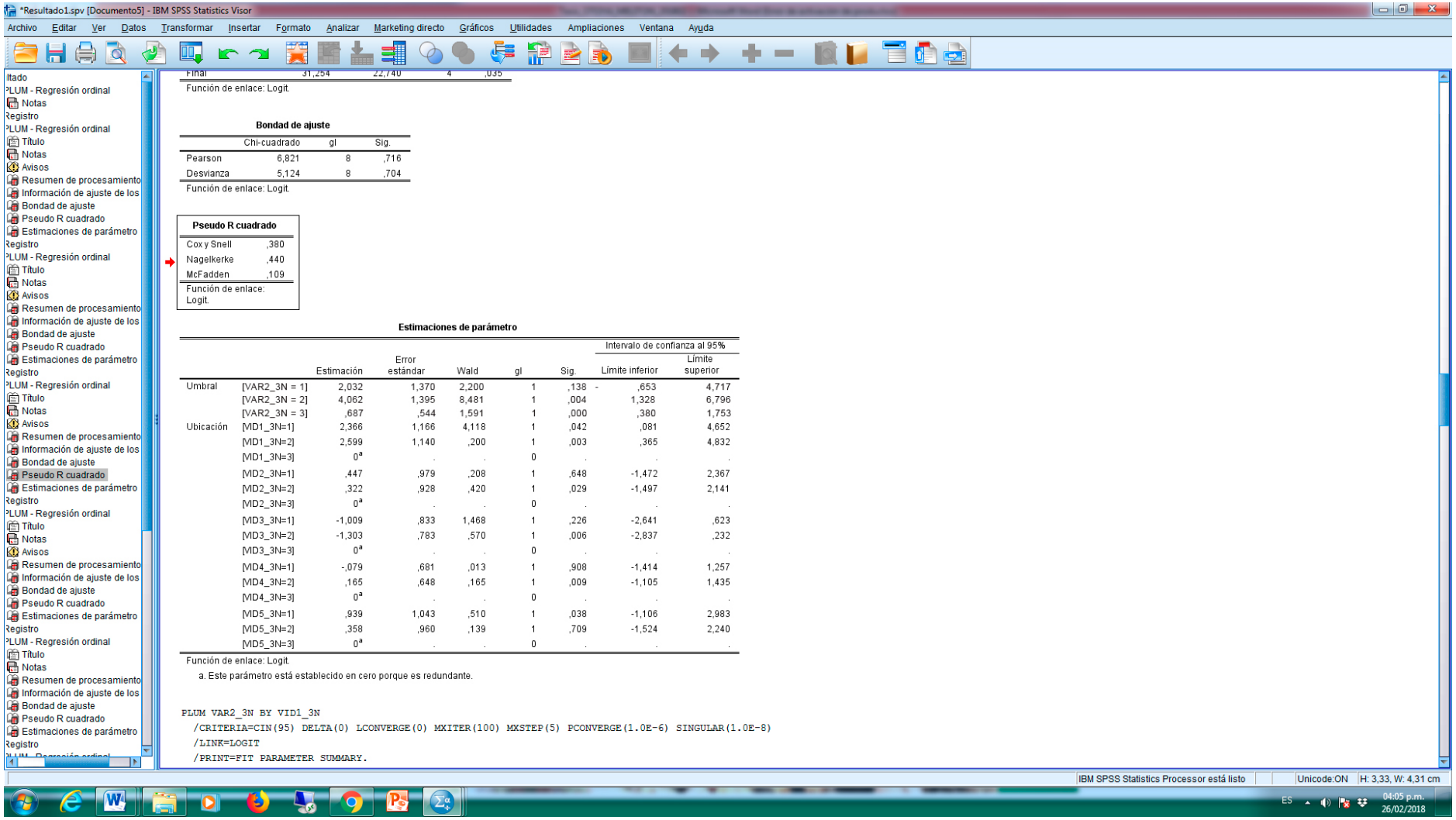
Cox y Snell	,380
Nagelkerke	,440
McFadden	,109

Función de enlace: Logit.

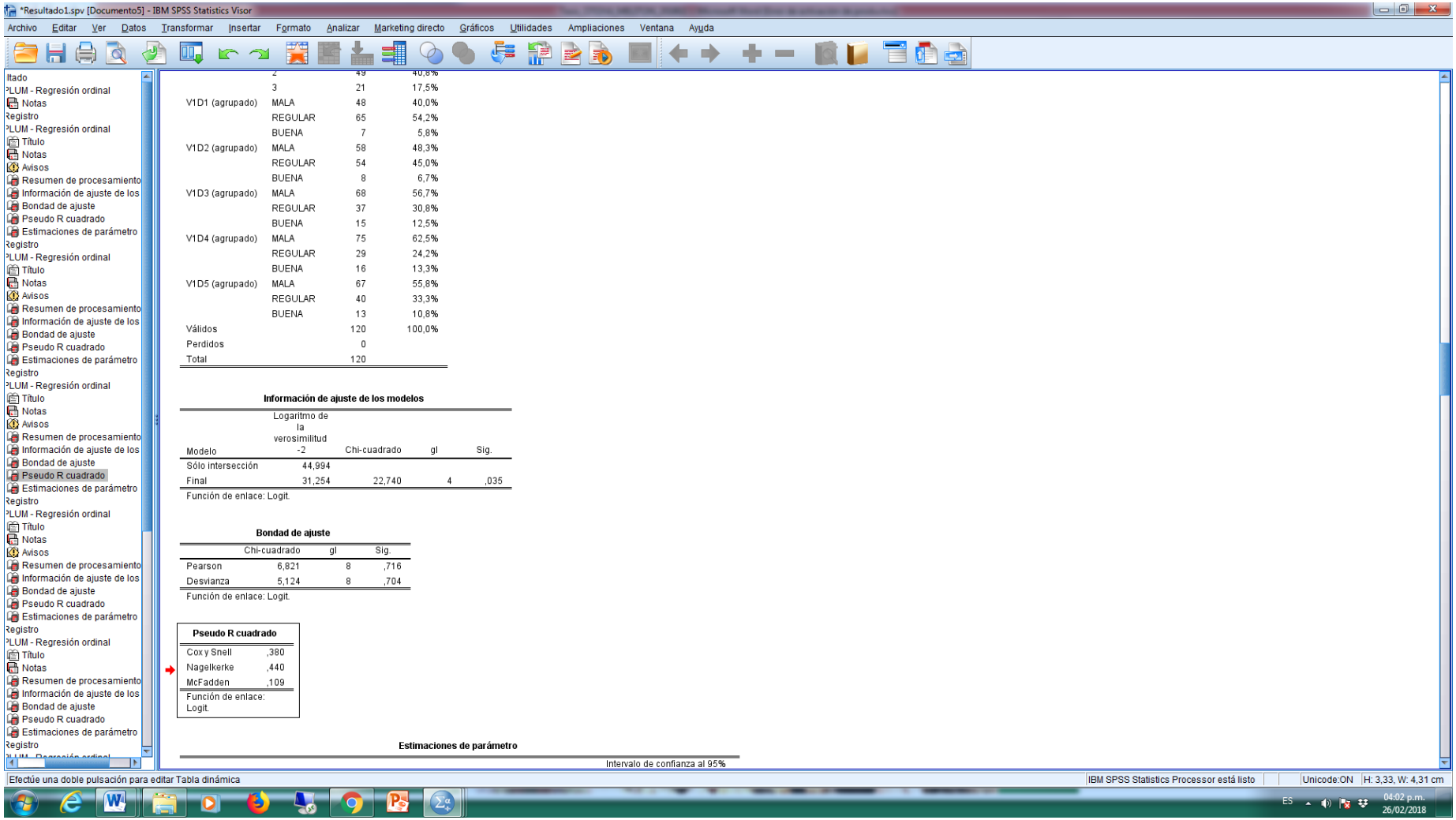
Estimaciones de parámetro

Intervalo de confianza al 95%

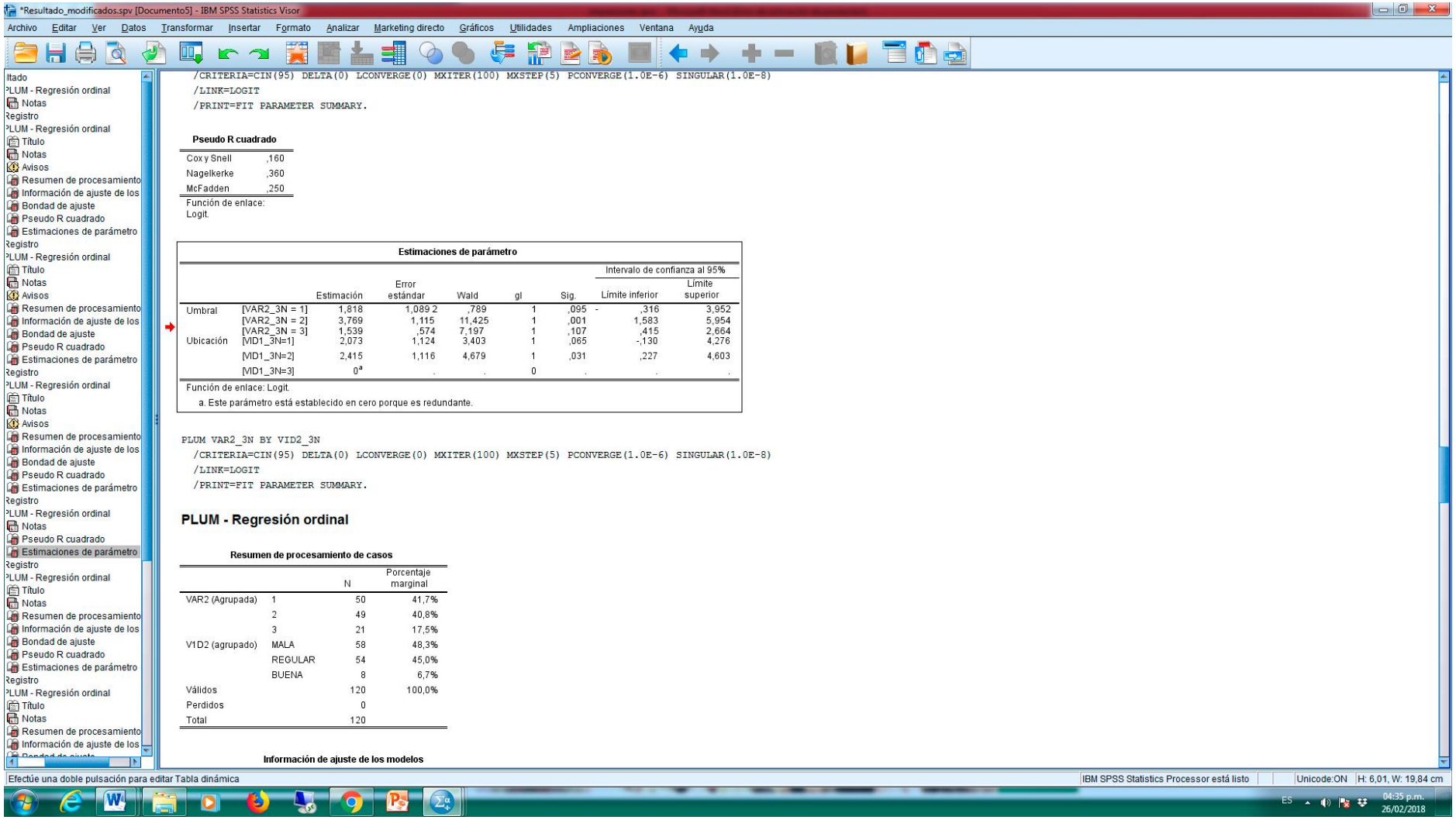
Estimación de parámetros de la gestión de riesgos en la seguridad de la información de Agrorural.



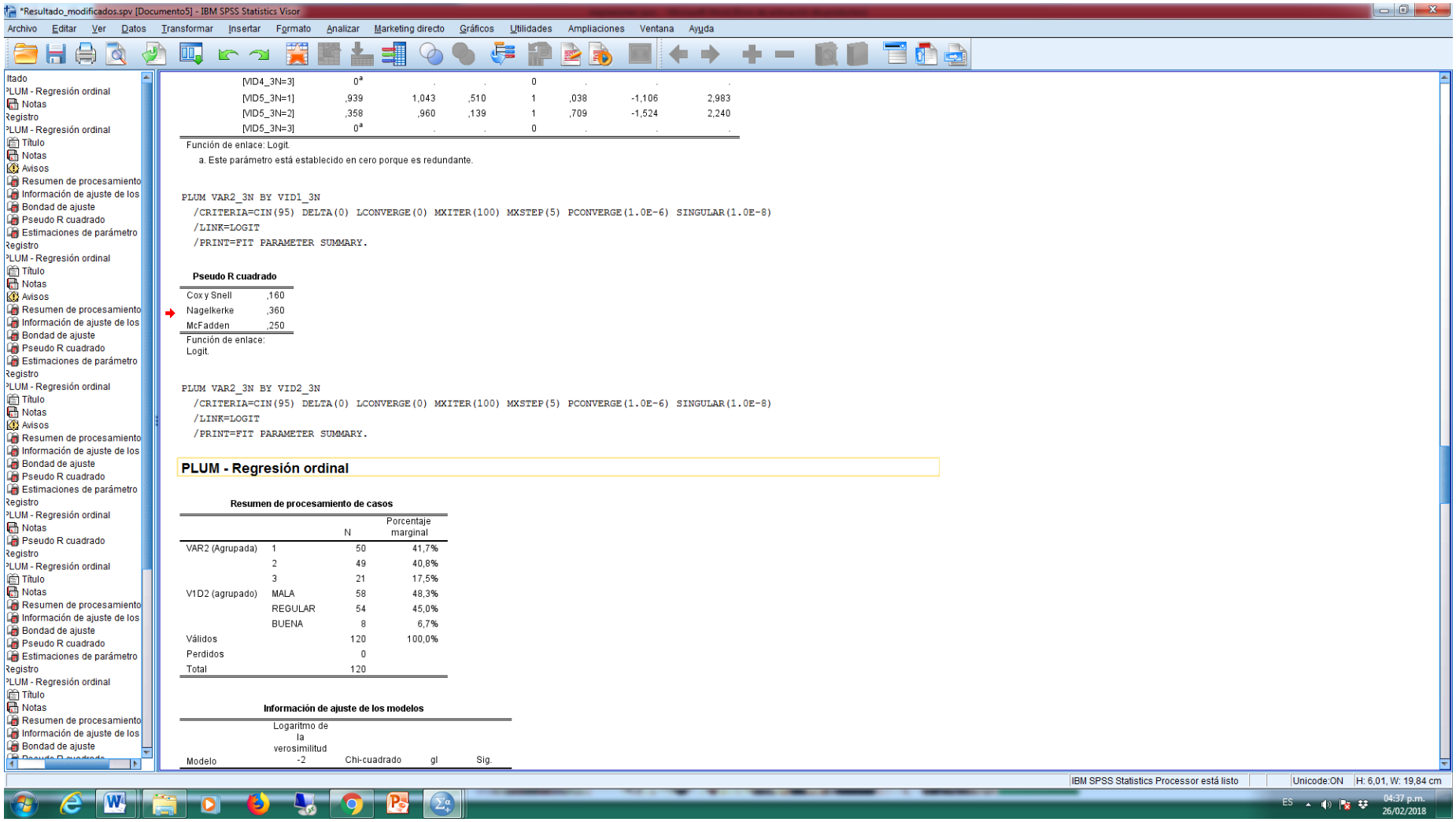
Coeficientes de la gestión de riesgos en la seguridad de la información de Agrorural, prueba de hipótesis general.



Resultado específico 1: Estimación de parámetros de los activos de información en la seguridad de la información.



Pseudo coeficiente de determinación de la dimensión de los activos de información en la seguridad de la información, prueba de hipótesis 1.



*Resultado_modificados.spv [Documento5] - IBM SPSS Statistics Visor

Archivo Editar Ver Datos Transformar Insertar Formato Analizar Marketing directo Gráficos Utilidades Ampliaciones Ventana Ayuda

	[MD4_3N=3]	0[a]	.	.	0	.	.	.
	[MD5_3N=1]	,939	1,043	,510	1	,038	-1,106	2,983
	[MD5_3N=2]	,358	,960	,139	1	,709	-1,524	2,240
	[MD5_3N=3]	0[a]	.	.	0	.	.	.

Función de enlace: Logit.

a. Este parámetro está establecido en cero porque es redundante.

```
PLUM VAR2_3N BY VID1_3N
  /CRITERIA=CIN(95) DELTA(0) LCONVERGE(0) MXITER(100) MXSTEP(5) PCONVERGE(1.0E-6) SINGULAR(1.0E-8)
  /LINK=LOGIT
  /PRINT=FIT PARAMETER SUMMARY.
```

Pseudo R cuadrado

Cox y Snell	,160
Nagelkerke	,360
McFadden	,250

Función de enlace: Logit.

```
PLUM VAR2_3N BY VID2_3N
  /CRITERIA=CIN(95) DELTA(0) LCONVERGE(0) MXITER(100) MXSTEP(5) PCONVERGE(1.0E-6) SINGULAR(1.0E-8)
  /LINK=LOGIT
  /PRINT=FIT PARAMETER SUMMARY.
```

PLUM - Regresión ordinal

Resumen de procesamiento de casos

		N	Porcentaje marginal
VAR2 (Agrupada)	1	50	41,7%
	2	49	40,8%
	3	21	17,5%
V1D2 (agrupado)	MALA	58	48,3%
	REGULAR	54	45,0%
	BUENA	8	6,7%
Válidos		120	100,0%
Perdidos		0	
Total		120	

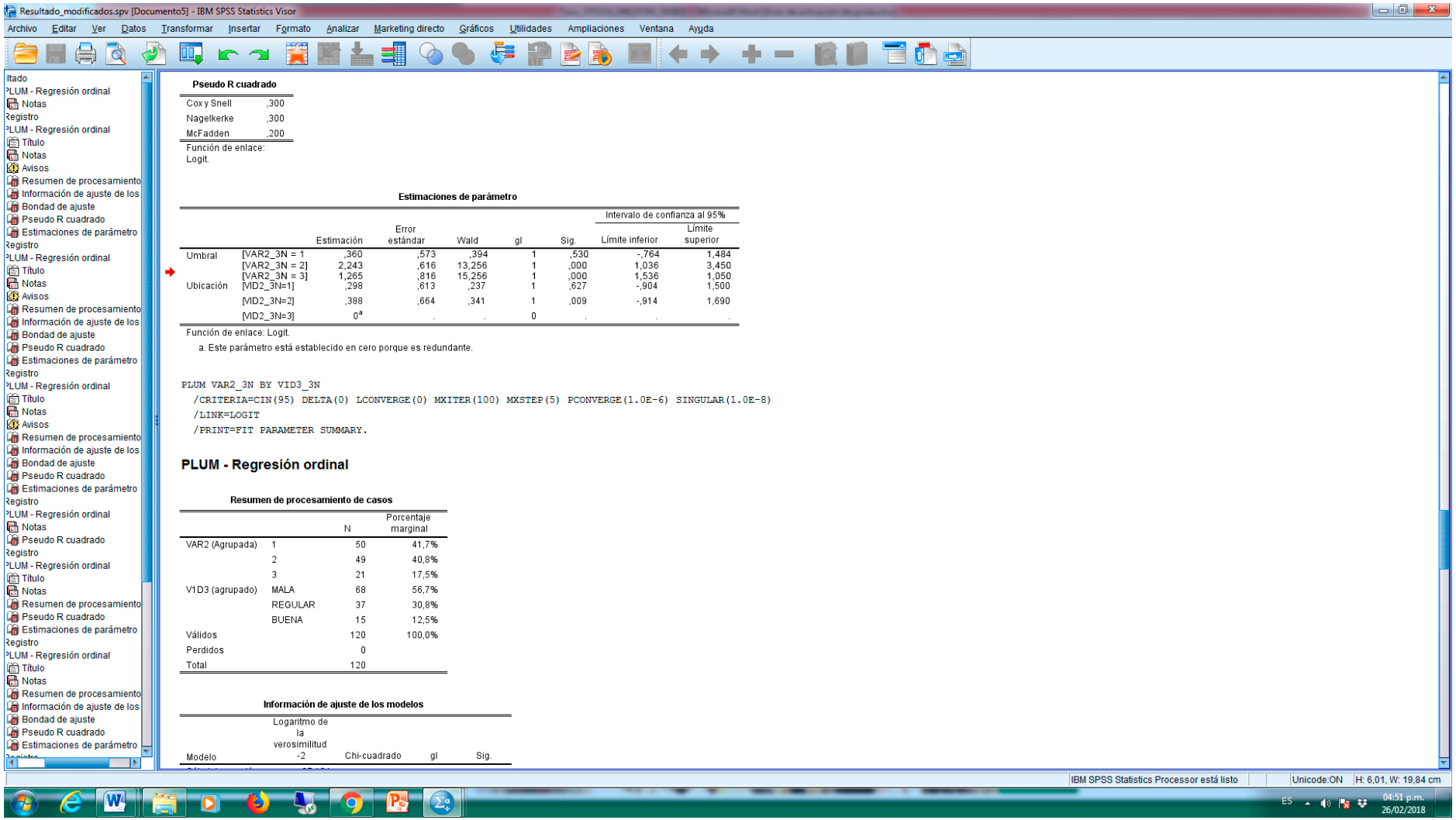
Información de ajuste de los modelos

Modelo	Logaritmo de la verosimilitud -2	Chi-cuadrado	gl	Sig.

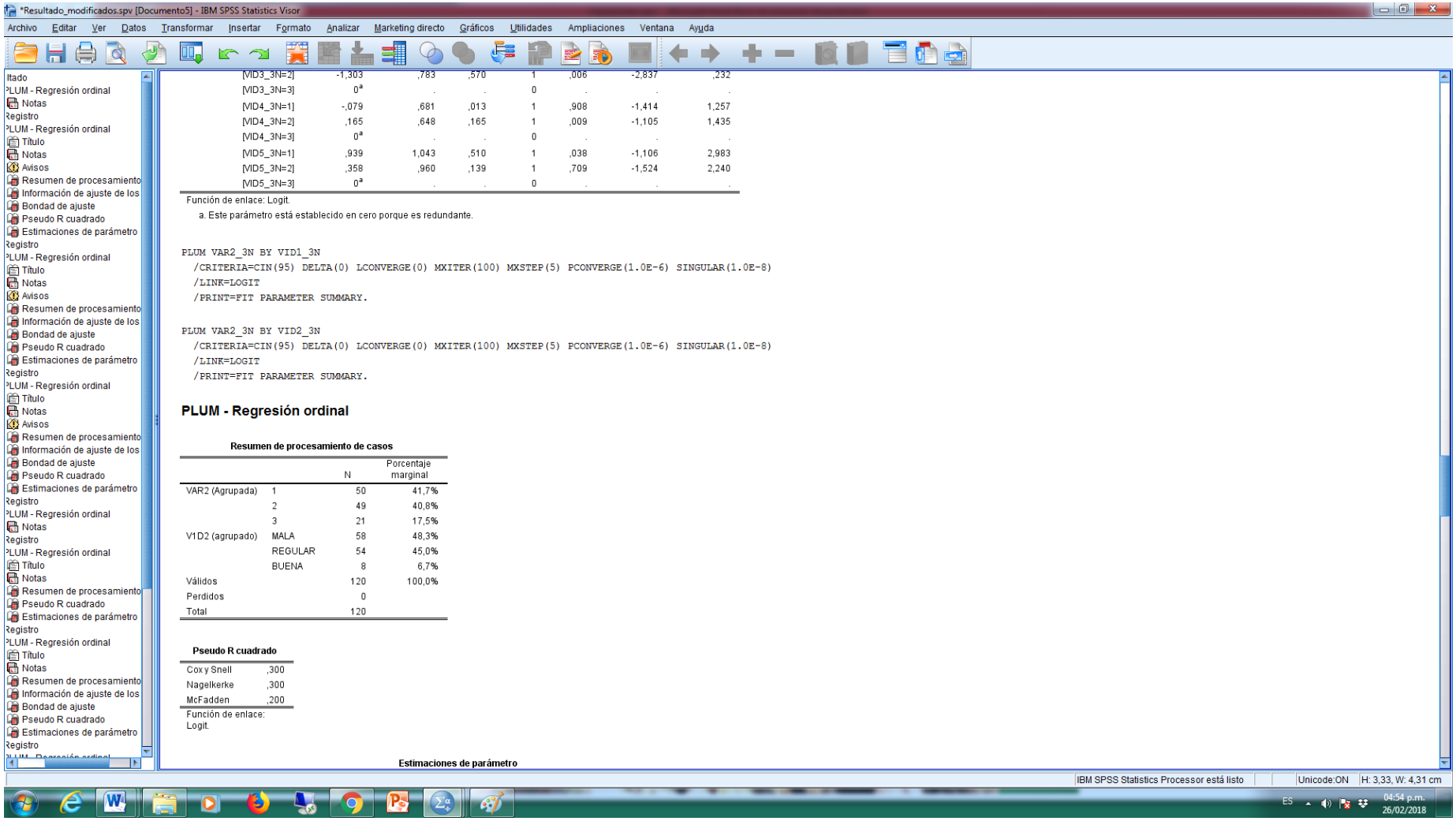
IBM SPSS Statistics Processor está listo | Unicode:ON | H: 6,01, W: 19,84 cm

ES 04:37 p.m. 26/02/2018

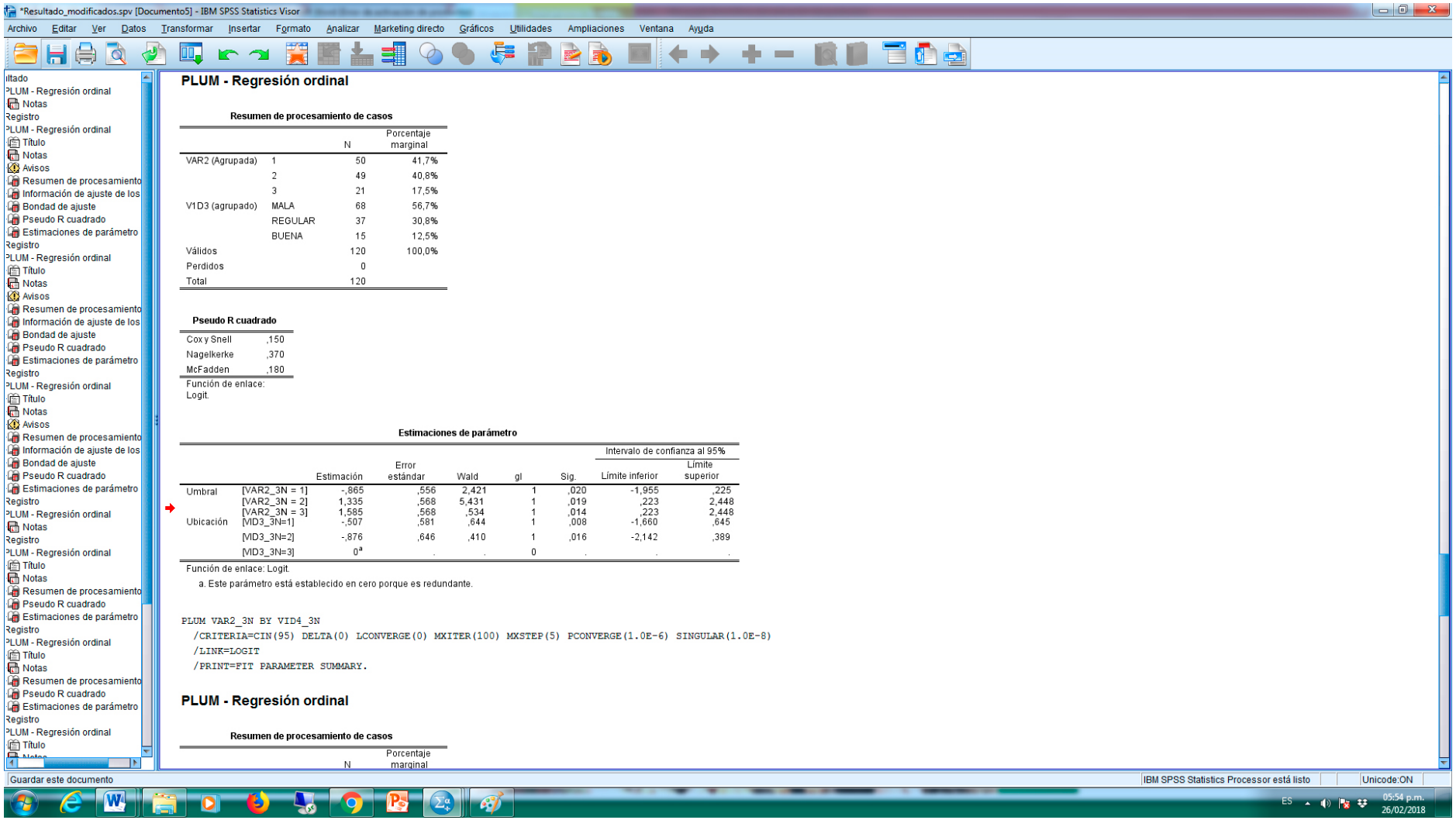
Resultado específico 2: Estimación de parámetros de las amenazas de los activos de información en la seguridad de la información



Pseudo coeficiente de determinación de la dimensión amenazas en la seguridad de la información, prueba de hipótesis 2



Resultado específico 3: Estimación de parámetros del impacto potencial de ejecución de las amenazas en la seguridad de la información



Resumen de procesamiento de casos

		N	Porcentaje marginal
VAR2 (Agrupada)	1	50	41,7%
	2	49	40,8%
	3	21	17,5%
V1D3 (agrupado)	MALA	68	56,7%
	REGULAR	37	30,8%
	BUENA	15	12,5%
Válidos		120	100,0%
Perdidos		0	
Total		120	

Pseudo R cuadrado

Cox y Snell	,150
Nagelkerke	,370
McFadden	,180

Función de enlace: Logit.

Estimaciones de parámetro

		Estimación	Error estándar	Wald	gl	Sig.	Intervalo de confianza al 95% Límite inferior	Límite superior
Umbral	[VAR2_3N = 1]	-,865	,556	2,421	1	,020	-1,955	,225
	[VAR2_3N = 2]	1,335	,568	5,431	1	,019	,223	2,448
	[VAR2_3N = 3]	1,585	,568	,534	1	,014	,223	2,448
Ubicación	[VID3_3N=1]	-,507	,581	,644	1	,008	-1,660	,645
	[VID3_3N=2]	-,876	,646	,410	1	,016	-2,142	,389
	[VID3_3N=3]	0[a]	.	.	0	.	.	.

Función de enlace: Logit.

a. Este parámetro está establecido en cero porque es redundante.

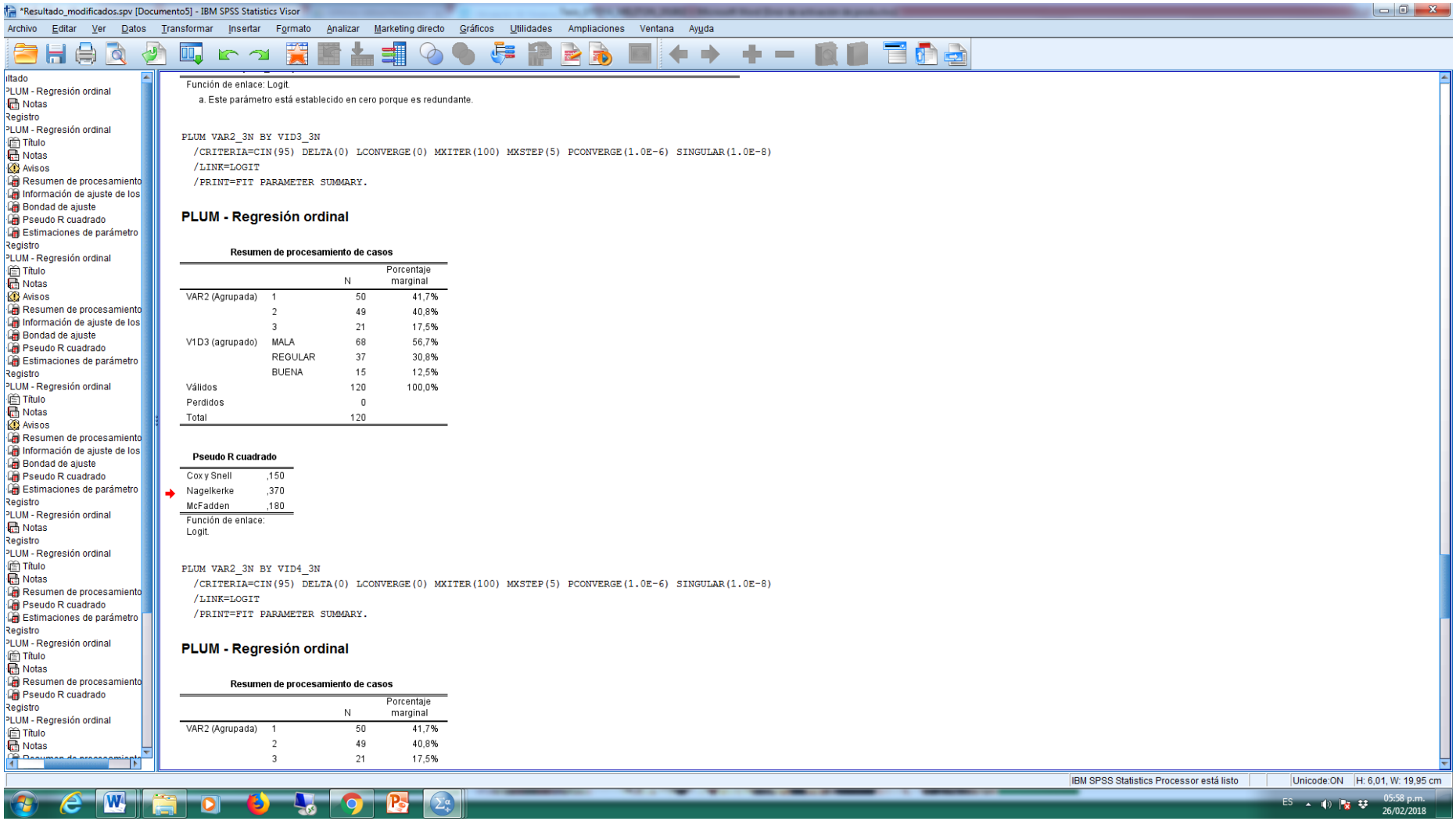
```
PLUM VAR2_3N BY VID4_3N
  /CRITERIA=CIN(95) DELTA(0) LCONVERGE(0) MXITER(100) MXSTEP(5) PCONVERGE(1.0E-6) SINGULAR(1.0E-8)
  /LINK=LOGIT
  /PRINT=FIT PARAMETER SUMMARY.
```

PLUM - Regresión ordinal

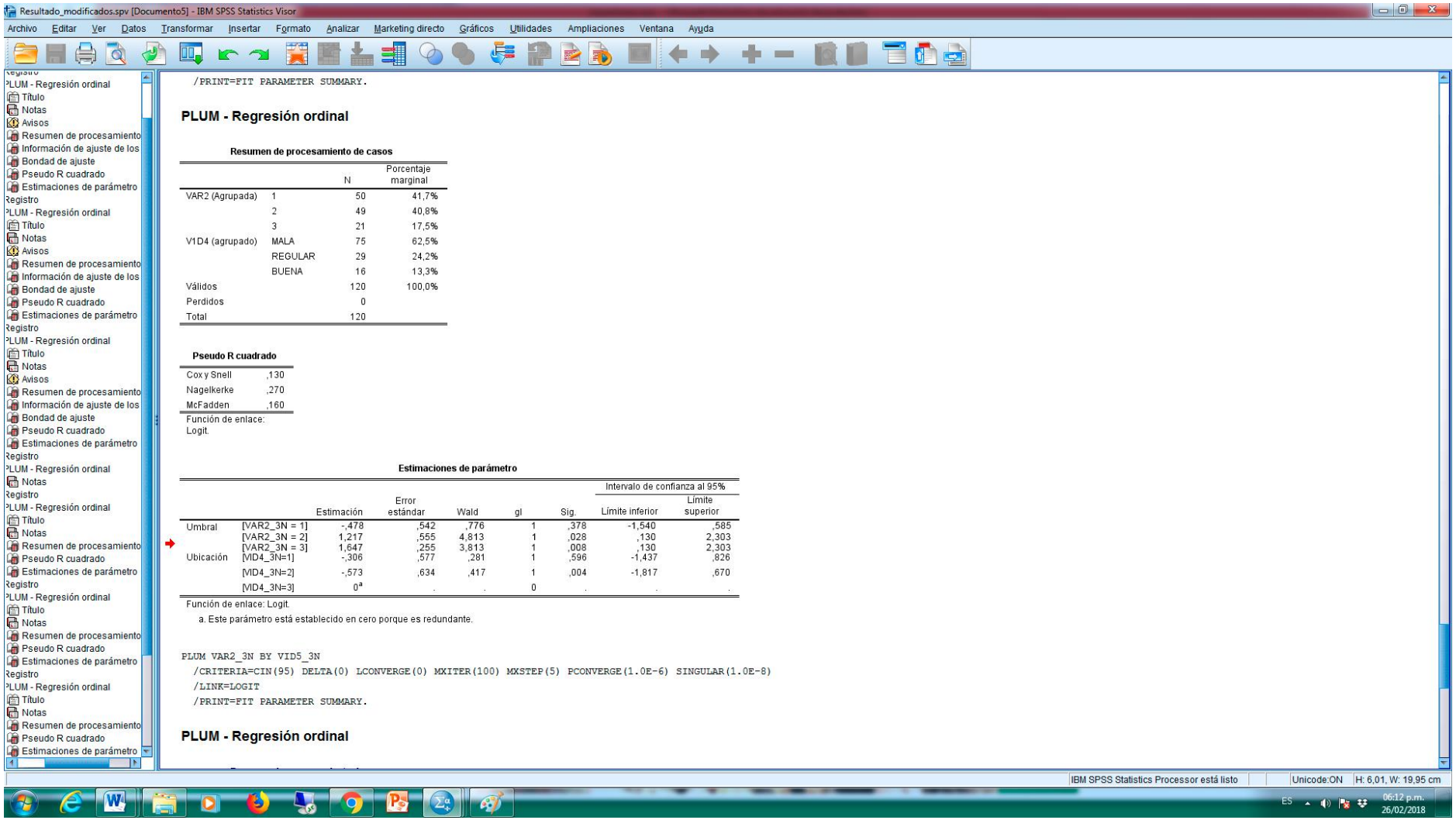
Resumen de procesamiento de casos

		N	Porcentaje marginal

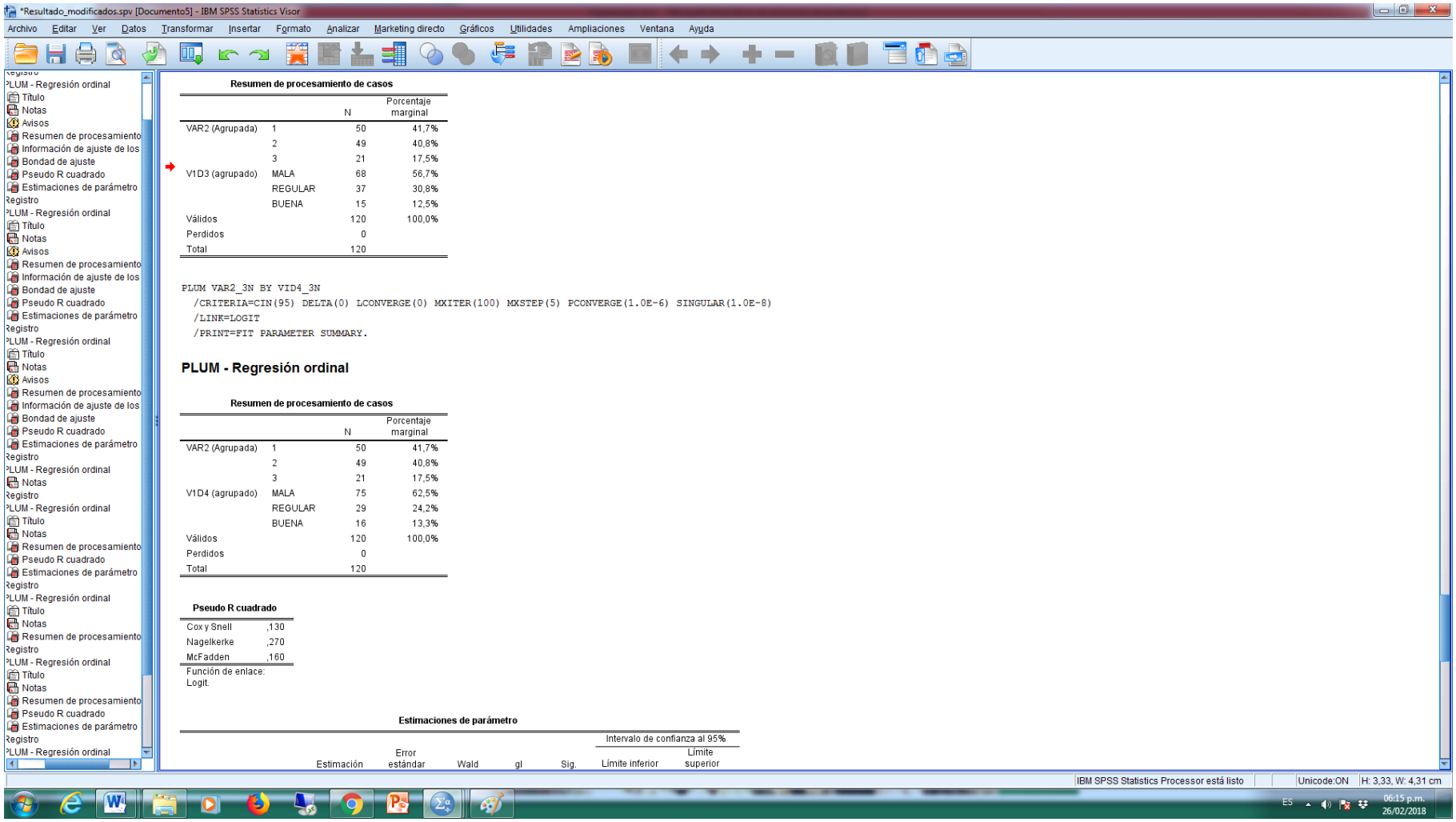
Pseudo coeficiente de la dimensión impacto potencial de ejecución de amenazas en la seguridad de la información, prueba de hipótesis 3



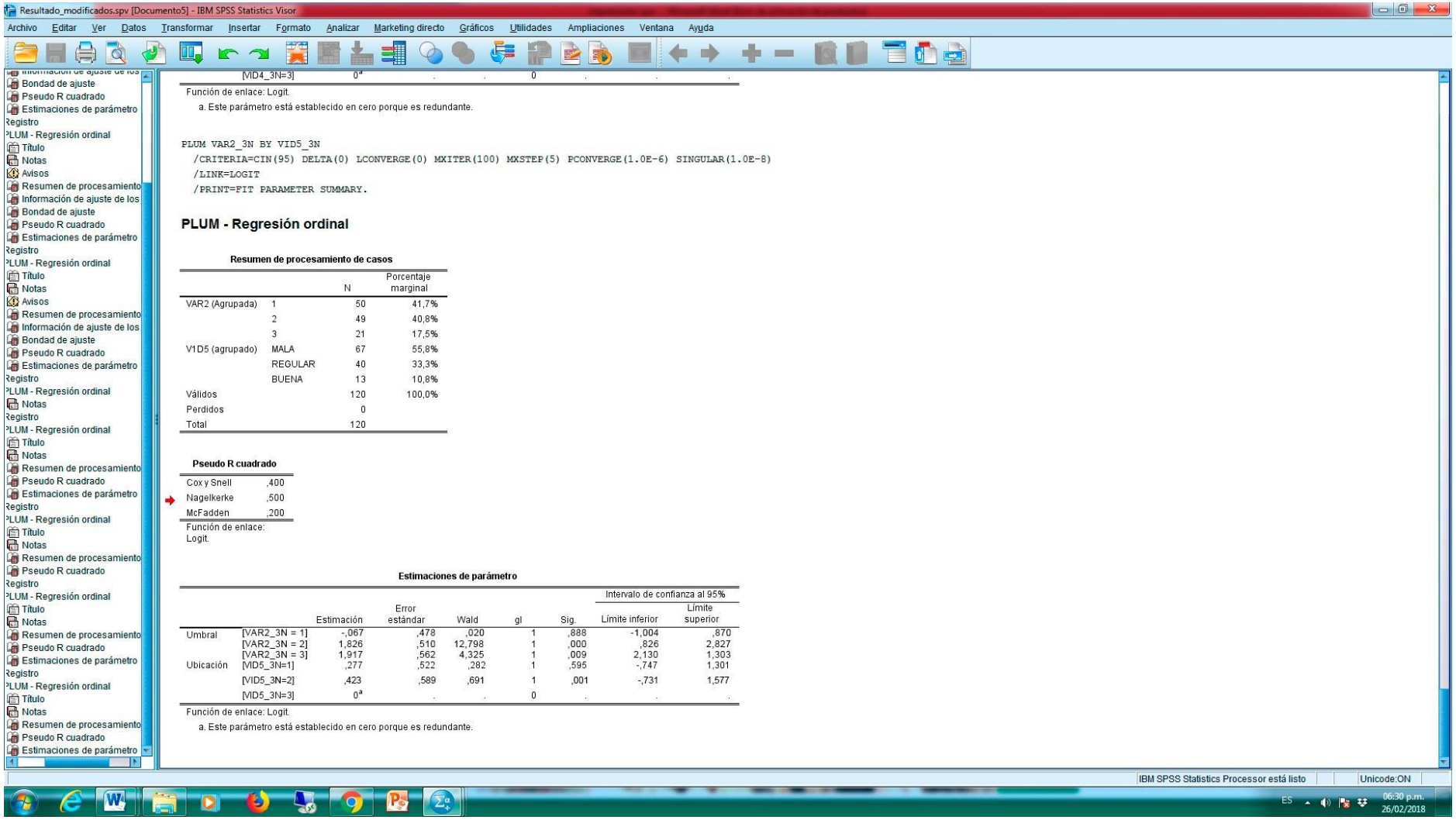
Resultado específico 4: Estimación de parámetros del riesgo potencial de ejecución de las amenazas en la seguridad de la información



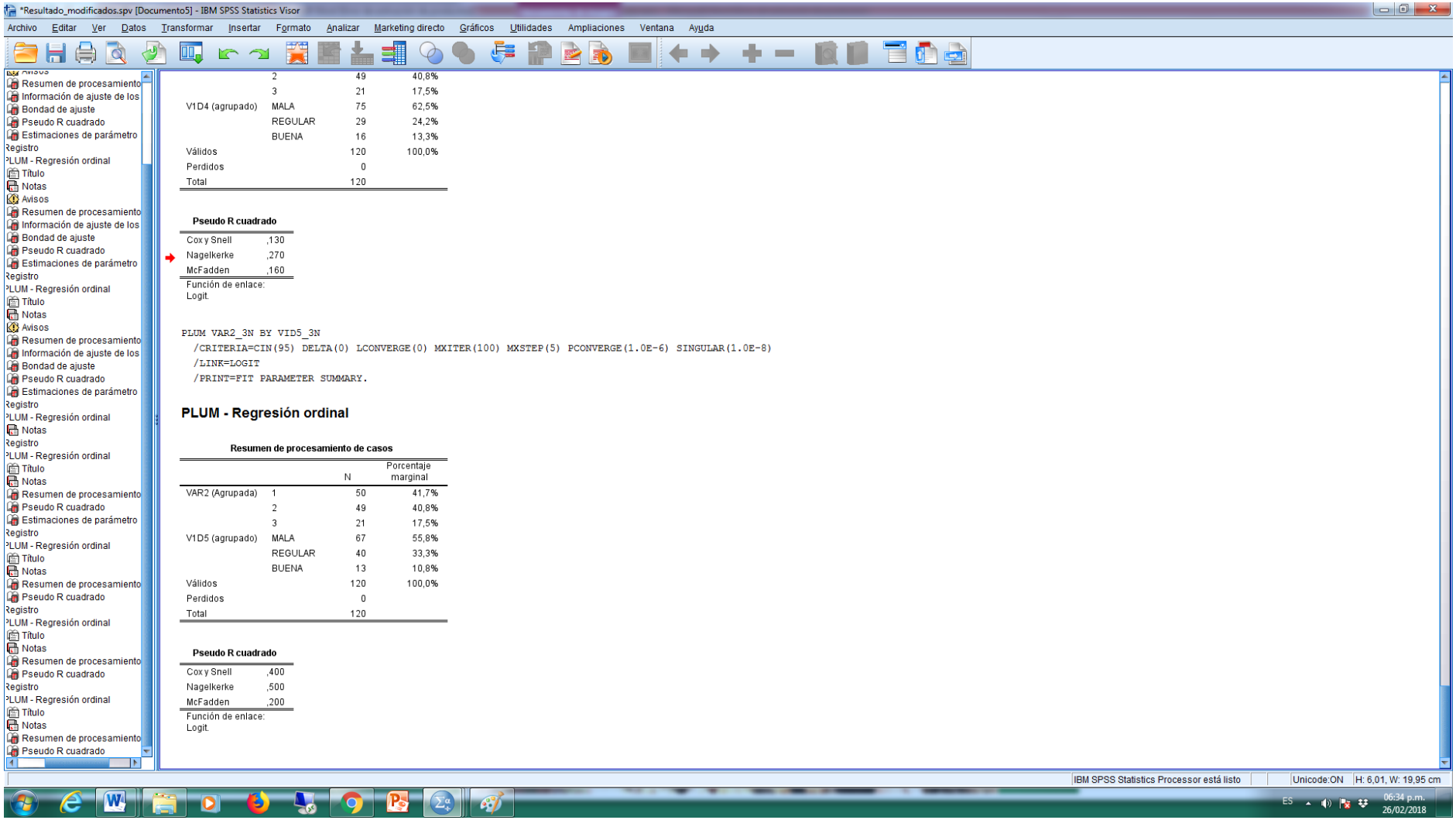
Pseudo coeficiente de la dimensión riesgo potencial de ejecución de amenazas en la seguridad de la información, prueba de hipótesis 4



Resultado específico 5: Estimación de parámetros de salvaguardas en la seguridad de la información



Pseudo coeficiente de la dimensión de salvaguardas en la seguridad de la información, prueba de hipótesis 5



ESCUELA DE POSGRADO
UNIVERSIDAD CÉSAR VALLEJO

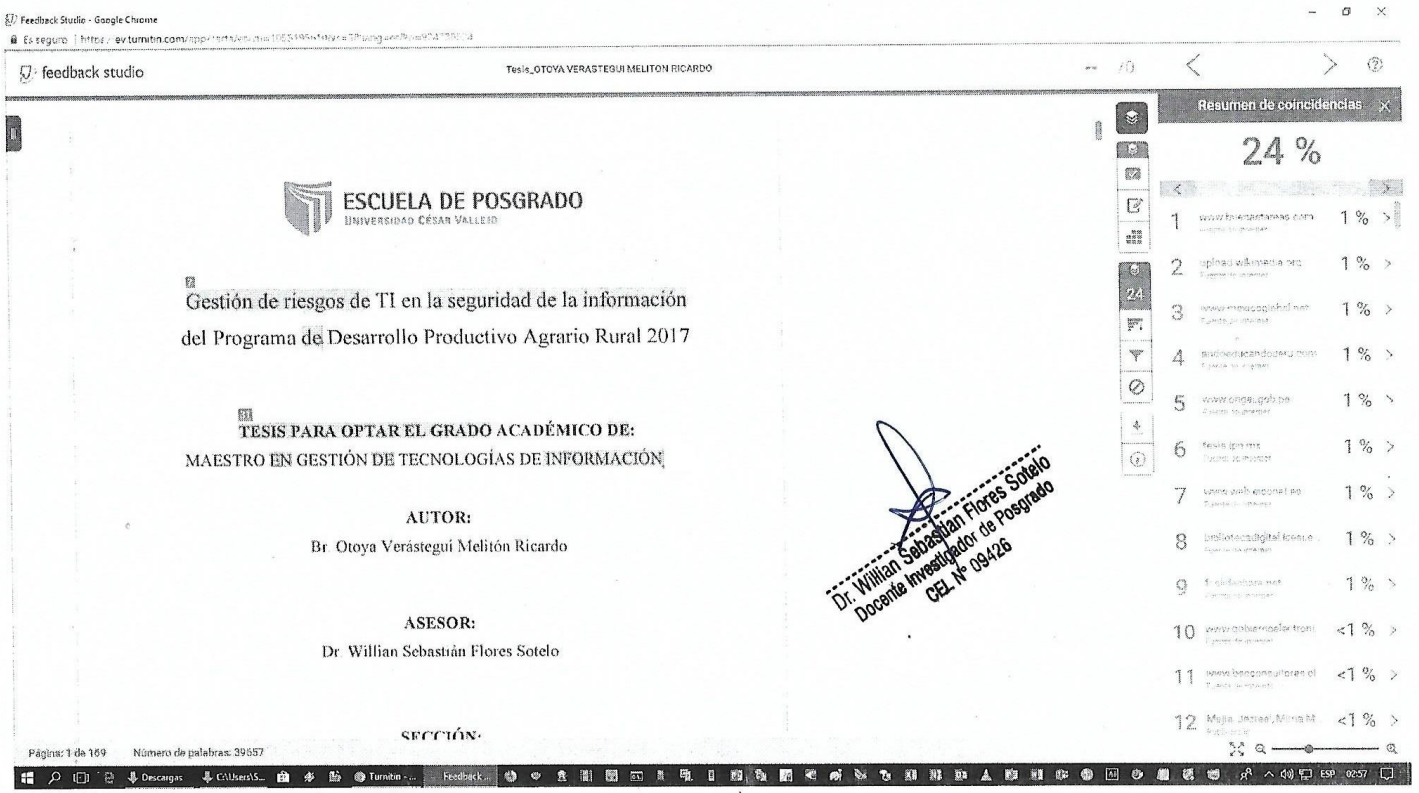
Acta de Aprobación de originalidad de Tesis

Yo, Willian Sebastián Flores Sotelo, docente de la Escuela de Posgrado de la UCV y revisor del trabajo académico titulado "Gestión de riesgos de TI en la seguridad de la información del Programa de Desarrollo Productivo Agrario Rural 2017" del estudiante Melitón Ricardo Otoya Verástegui; y habiendo sido capacitado e instruido en el uso de la herramienta Turnitin, he constatado lo siguiente:

Que el citado trabajo académico tiene un índice de similitud constato 24% verificable en el reporte de originalidad del programa turnitin, grado de coincidencia mínimo que convierte el trabajo en aceptable y no constituye plagio, en tanto cumple con todas las normas del uso de citas y referencias establecidas por la universidad César Vallejo.

Olivos, 04 de Marzo del 2018

Willian Sebastián Flores Sotelo
DNI: 06175729



Feedback Studio - Google Chrome

feedback studio — Tesis_OTOYA VERASTEGUI MELITON RICARDO

Resumen de coincidencias

24 %

1		1 %
2		1 %
3		1 %
4		1 %
5		1 %
6		1 %
7		1 %
8		1 %
9		1 %
10		<1 %
11		<1 %
12		<1 %

ESCUELA DE POSGRADO
UNIVERSIDAD CÉSAR VALLEJO

Gestión de riesgos de TI en la seguridad de la información del Programa de Desarrollo Productivo Agrario Rural 2017

TESIS PARA OPTAR EL GRADO ACADÉMICO DE:
MAESTRO EN GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN

AUTOR:
Br. Otoya Verástegui Melitón Ricardo

ASESOR:
Dr. Willian Sebastián Flores Sotelo

SECCIÓN:

Dr. Willian Sebastián Flores Sotelo
Docente Investigador de Posgrado
CEL N° 09426

Página: 1 de 169 Número de palabras: 39657

UNIVERSIDAD CÉSAR VALLEJO

Centro de Recursos para el Aprendizaje y la Investigación (CRAI)
"César Acuña Peralta"

FORMULARIO DE AUTORIZACIÓN PARA LA PUBLICACIÓN ELECTRÓNICA DE LAS TESIS

1. DATOS PERSONALES

Apellidos y Nombres: (solo los datos del que autoriza)
OTOYA VERASTEGUI MELITON RICARDO
D.N.I. : 19336295
Domicilio : URB. JARDINES NORAMTALI II ETAPA M7. C 11.16 S.M.P.
Teléfono : Fijo : ..... Móvil 955482370
E-mail : ricardoetaya@hotmail.com

2. IDENTIFICACIÓN DE LA TESIS

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

☒ Tesis de Posgrado
☒ Maestría ☐ Doctorado
Grado : MAESTRO
Mención : GESTION DE TECNOLOGÍAS DE INFORMACION

3. DATOS DE LA TESIS

Autor (es) Apellidos y Nombres: OTOYA VERÁSTEGUI MELITON RICARDO

Título de la tesis: "GESTION DE RIESGOS DE T.I. EN LA SEGURIDAD DE LA INFORMACION DEL PROGRAMA DE DESARROLLO PRODUCTIVO AGRARIO RURAL 2017."

Año de publicación : 2018

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

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

Firma : ..... Fecha: 04/07/2018.

ESCUELA DE POSGRADO
UNIVERSIDAD CÉSAR VALLEJO

William Flores 1034-78

FORMATO DE SOLICITUD

SOLICITA: V.B EMPASTE DE TESIS

ESCUELA DE POSGRADO

MELITON RICARDO OTOYA VERASTEGUI con DNI N° 19836295
(Nombres y apellidos del solicitante) (Número de DNI)

domiciliado (a) en URB. JARDINES DE NARANJAL II ETAPA MZ. "C" LOTE 16
(Calle / Lote / Mz. / Urb. / Distrito / Provincia /Región)

ante Ud. con el debido respeto expongo lo siguiente:

Que en mi condición de alumno de la promoción: 2018 del programa: POSTGRADO - MAESTRIA EN GESTION DE LAS TIC identificado con el código de matrícula N° 6000141105
(Promoción) (Nombre del programa) (Código de alumno)

de la Escuela de Posgrado, recurro a su honorable despacho para solicitarle lo siguiente:

VISTO BUENO PARA EMPASTE DE MI TESIS: "GESTION DE RIESGOS DE TI EN LA SEGURIDAD DE LA INFORMACION DEL PROGRAMA PRODUCTIVO AGRARIO RURAL 2017

Por lo expuesto, agradeceré ordenar a quien corresponde se me atienda mi petición por ser de justicia.

Lima, 21 de JUNIO de 2018

ESCUELA DE POSGRADO UNIVERSIDAD CÉSAR VALLEJO
CAMPUS LIMA NORTE
OFICINA DE INVESTIGACIÓN
21 JUN. 2018
RECIBIDO

(Firma del solicitante)

Documentos que adjunto:
a. COPIA RESOLUCION DIRECTORAL N° 1162-2018
b. COPIA DICTAMEN SUSTENTACION TESIS
c. ACTA DE APROBACION ORIGINAL (DE TESIS)
d. PANTALLAZO DE TURNITIN 6

Cualquier consulta por favor comunicarse conmigo al:
Teléfonos: 955482370
Email: ricardootoya@hotmail.com

ESCUELA DE POSGRADO UCV INVESTIGACIÓN CAMPUS LIMA NORTE

Dr. Willian Sebastián Flores Sotelo
Docente Investigador de Posgrado
CEL N° 09426

VB para publicacion