



**FACULTAD DE INGENIERÍA,
ARQUITECTURA Y URBANISMO**

**ESCUELA PROFESIONAL DE
INGENIERÍA DE SISTEMAS**

TESIS

**INFLUENCIA DE LA METODOLOGÍA MAGERIT
V3 EN LA SEGURIDAD DE INFORMACIÓN DE LA
EMPRESA DECO INTERIORS SAC.**

**PARA OPTAR EL TÍTULO PROFESIONAL DE
INGENIERO DE SISTEMAS**

Autor:

Bach. Cabrejos Torres Ramiro

ORCID: <https://orcid.org/0000-0003-3329-5557>

Asesor(a):

Mg. Atalaya Urrutia Carlos William

ORCID: <https://orcid.org/0000-0002-2761-4868>

Línea de Investigación:

Infraestructura, Tecnología y Medio Ambiente

Pimentel – Perú

2020

**INFLUENCIA DE LA METODOLOGÍA MAGERIT V3 EN LA SEGURIDAD DE
INFORMACIÓN DE LA EMPRESA DECO INTERIORS SAC.**

APROBACIÓN DE LA TESIS

Dr.

Asesor Metodológico

Dr.

Presidente del jurado de tesis

Secretaria del jurado de tesis

Vocal del jurado de tesis

DEDICATORIAS

Dedico esta tesis primeramente a Dios por guiarme y bendecirme en este recorrido de mi vida.

A mis padres Adela y Ramiro, por su amor, esfuerzo y sacrificio, a lo largo de todos estos años, infinitas gracias porque siempre creyeron en mí, entregándome su apoyo incondicional.

A mi hijo Mateo, mi mayor motivación y origen de mi esfuerzo, para ser una mejor persona y profesional.

A mi esposa Melissa, por ser mi complemento, gracias a su confianza, apoyo y comprensión.

A mis hermanas, Daniela y Senne, por estar siempre presentes en mi vida a pesar de la distancia, además de darme unos hermosos sobrinos; Cielo, Brissa, Gabriel y Gía; quienes forman parte de mi motivación.

A toda mi familia, abuelos, tíos, primos, sobrinos, suegros, cuñados, amigos del BF y en especial a mis padrinos quienes con su apoyo y consejos me ayudaron a lograr una meta más en mi vida, gracias por inculcar en mí los mejores ejemplos de dedicación y sacrificio para luchar por lo que he querido.

Para ustedes infinitas gracias.

Ramiro Cabrejos Torres.

AGRADECIMIENTOS

A Dios por permitirme vivir y lograr mis sueños.

A mi familia por su ejemplo de constancia.

A la Universidad Señor de Sipán por abrirme sus puertas y permitirme cumplir mi meta.

A mis profesores que guiaron mi camino hasta este momento.

Siempre les estaré eternamente agradecido.

Ramiro Cabrejos Torres.

TABLA DE CONTENIDO

DEDICATORIAS.....	III
AGRADECIMIENTOS.....	IV
RESUMEN.....	XII
ABSTRACT	XIII
I. INTRODUCCIÓN.....	14
1.1. Planteamiento del problema.....	14
1.2. Antecedentes de estudio	16
1.3. Abordaje teórico (Marco Teórico)	21
1.3.1. Teorías relacionadas al tema.....	21
1.3.2. Marco Conceptual.....	31
1.4. Formulación del Problema.....	33
1.4.1. Problema General	33
1.5. Justificación e importancia del estudio.....	33
1.6. Hipótesis.	33
1.7. Objetivos	34
1.7.1. Objetivos General	34
1.7.2. Objetivos Específicos	34
1.8. Limitaciones.....	34
II. MATERIAL Y MÉTODO.....	35
2.1. Tipo y Diseño de Investigación.....	35
2.2. Población y muestra.....	35
2.3. Variables, Operacionalización.....	36
2.3.1. Variable independiente: Metodología MAGERIT	36
2.3.2. Variable dependiente: Seguridad de la información	36
2.3.3. Operacionalización de las variables	6
2.4. Técnicas e instrumentos de recaudación de datos, validez y confiabilidad.....	6
2.5. Procedimientos de análisis de datos.....	10
2.6. Criterios éticos	10
2.7. Criterios de Rigor científico.....	11
III. RESULTADOS.....	12
3.1. Análisis descriptivo.....	12
3.1.1. Análisis de normalidad.....	40
3.1.2. Prueba de hipótesis.....	40
3.2. Discusión de resultados	43
3.3. Aporte práctico	45
3.3.1. Fundamentación del aporte práctico.....	45
3.3.2. Construcción del aporte práctico.....	46
3.3.3. Creación del proyecto en PILAR	47
3.3.4. Caracterización de los activos	47
3.3.5. Caracterización de las amenazas.....	55
3.3.6. Caracterización de las Salvaguardas.....	59
3.3.7. Estimación del Estado de Riesgo	62
3.3.8. Proceso de Gestión de los Riesgos.....	72
3.3.9. Plan de Tratamiento de Riesgos	88

3.4.	Valoración y corroboración de los Resultados	99
3.4.1.	Valoración de los resultados (criterio de expertos)	99
3.4.2.	Corroboración estadística de las transformaciones logradas	99
IV.	CONCLUSIONES.....	100
V.	RECOMENDACIONES	101
VI.	REFERENCIAS.....	102
VII.	ANEXOS	108
	ANEXO N° 1. MATRIZ DE CONSISTENCIA	109
	ANEXO N° 2. OPERACIONALIZACIÓN DE LAS VARIABLES	111
	ANEXO N° 3 INSTRUMENTO.....	113
	ANEXO N° 4 INSTRUMENTO DE VALIDACION NO EXPERIMENTAL POR JUICIO DE EXPERTOS.....	129
	ANEXO N° 5 VALIDACIÓN DEL APOORTE PRÁCTICO DE LA INVESTIGACIÓN ENCUESTA A EXPERTOS.....	141
	ANEXO N° 6 IDENTIFICACIÓN DE ACTIVOS	149
	ANEXO N° 7 VALORACIÓN DE ACTIVOS	150
	ANEXO N° 8 IDENTIFICACIÓN DE AMENAZAS.....	151
	ANEXO N° 9 VALORACION DE AMENAZAS.....	168
	ANEXO N° 10 IDENTIFICACIÓN Y VALORACION DE SALVAGUARDAS	186
	ANEXO N° 11 RIESGO POTENCIAL DE LOS ACTIVOS	187
	ANEXO N° 12 RIESGO RESIDUAL DE LOS ACTIVOS	189
	ANEXO N° 13 IMPACTO POTENCIAL SOBRE CADA UNO DE LOS ACTIVOS.....	191
	ANEXO N° 14 IMPACTO RESIDUAL	193
	ANEXO N° 15 PERMISO PARA LA RECOLECCIÓN DE DATOS.....	195
	ANEXO N° 16 RESOLUCIÓN DE APROBACIÓN DE PROYECTO DE INVESTIGACIÓN	196
	ANEXO N° 17 MODIFICACIÓN DE TÍTULO DE PROYECTO DE TESIS	197

TABLAS

TABLA 1. OPERACIONALIZACIÓN DE LA VARIABLE INDEPENDIENTE METODOLOGÍA MAGERIT V3.....	6
TABLA 2. TABLA DE OPERACIONALIZACIÓN DE LA VARIABLE DEPENDIENTE SEGURIDAD DE LA INFORMACIÓN DE LA EMPRESA DECO INTERIORS	7
TABLA 3. CONFIABILIDAD.....	8
TABLA 4. RESUMEN DE PROCESAMIENTO DE CASOS DE LA VARIABLE 1	8
TABLA 5. ESTADÍSTICA DE FIABILIDAD DE LA VARIABLE 1	8
TABLA 6. RESUMEN DE PROCESAMIENTO DE CASOS DE LA VARIABLE 2	9
TABLA 7. ESTADÍSTICA DE FIABILIDAD DE LA VARIABLE 2	9
TABLA 8. RESUMEN DE PROCESAMIENTO DE CASOS DE LAS VARIABLES 1 Y 2.....	9
TABLA 9. ESTADÍSTICA DE FIABILIDAD DE LAS VARIABLES 1 Y 2	10
TABLA 10. ¿LA EMPRESA LE HA PROPORCIONADO CAPACITACIÓN SOBRE EL RESGUARDO DE LA INFORMACIÓN QUE ADMINISTRA?.....	12
TABLA 11. ÍTEM 2. ¿LA EMPRESA LE HA PROPORCIONADO INFORMACIÓN SOBRE LOS RIESGOS TECNOLÓGICOS DE LA INFORMACIÓN QUE ADMINISTRA?.....	14
TABLA 12. ÍTEM 3. ¿PONE EN PRÁCTICA ALGUNA ESTRATEGIA PARA LA PROTECCIÓN DE LA INFORMACIÓN?	15
TABLA 13. ÍTEM 4. ¿LA EMPRESA HA IMPLEMENTADO ALGUNA ESTRATEGIA PARA CONCIENTIZAR AL PERSONAL SOBRE LOS RIESGOS E IMPORTANCIA DE LOS ACTIVOS DE INFORMACIÓN?.....	16
TABLA 14. ÍTEM 5. ¿SE CONSIDERA COMPROMETIDO CON EL RESGUARDO DE LA INFORMACIÓN QUE ADMINISTRA?	17
TABLA 15. ÍTEM 6. ¿LA EMPRESA HA IMPLEMENTADO ALGUNA ESTRATEGIA PARA EVALUAR LOS RIESGOS A LOS QUE ESTÁ SOMETIDA LA INFORMACIÓN?	18
TABLA 16. ÍTEM 7. ¿LA EMPRESA HA DETERMINADO LOS RIESGOS A LOS QUE ESTÁN SOMETIDOS LOS ACTIVOS DE INFORMACIÓN?.....	19
TABLA 17. ÍTEM 8. ¿LA EMPRESA HA IDENTIFICADO LOS RIESGOS SOBRE LA INFORMACIÓN QUE AFECTARÍAN LAS LABORES DIARIAS?	20
TABLA 18. ÍTEM 9. ¿SE HAN CUANTIFICADO EN LA EMPRESA LOS POSIBLES DAÑOS EN LOS ACTIVOS DE INFORMACIÓN?	21
TABLA 19. ÍTEM 10. ¿LA TECNOLOGÍA DE INFORMACIÓN DISPONIBLE EN LA EMPRESA ES ADECUADA PARA EL DESARROLLO DE LAS ACTIVIDADES?	22
TABLA 20. ÍTEM 11. ¿LA TECNOLOGÍA DE INFORMACIÓN DISPONIBLE EN LA EMPRESA GARANTIZA LA SEGURIDAD DE LA INFORMACIÓN?	23
TABLA 21. ÍTEM 12. ¿EL SERVICIO DE INTERNET DISPONIBLE EN LA EMPRESA ES ADECUADO PARA LLEVAR A CABO SUS ACTIVIDADES?	24
TABLA 22. ÍTEM 13. ¿LAS COMPUTADORAS ESTÁN CONECTADAS CON LA RED PARA ENVIAR Y RECIBIR INFORMACIÓN?	25
TABLA 23. ÍTEM 14. ¿SU NIVEL DE PERICIA LE PERMITE REALIZAR UN ADECUADO ASEGURAMIENTO DE LA INFORMACIÓN QUE ADMINISTRA?	26
TABLA 24. ÍTEM 15. ¿REQUIERE DE ALGÚN TIPO DE ASISTENCIA PARA RESOLVER PROBLEMAS INFORMÁTICOS DURANTE SUS LABORES DIARIAS?.....	27
TABLA 25. ÍTEM 16. ¿EL SERVICIO DE INTERNET LE PERMITE INGRESAR A TODAS LAS PÁGINAS WEB QUE DESEE?	28
TABLA 26. ÍTEM 17. ¿PUEDE RECIBIR Y ENVIAR CORREOS DESDE SU COMPUTADORA DE TRABAJO?	29

TABLA 27. ÍTEM 18. ¿CONSIDERA QUE SU NIVEL DE CONOCIMIENTO EN EL MANEJO DE LA TECNOLOGÍA INFORMÁTICA, ES SÓLIDO?.....	30
TABLA 28. ÍTEM 19. ¿LA EMPRESA HA ESTABLECIDO POLÍTICAS O PROCEDIMIENTOS PARA ASEGURAR LA CONFIDENCIALIDAD DE LA INFORMACIÓN?	31
TABLA 29. ÍTEM 20. ¿LA EMPRESA HA ESTABLECIDO POLÍTICAS O PROCEDIMIENTOS PARA ASEGURAR LA INTEGRIDAD DE LA INFORMACIÓN?	32
TABLA 30. ÍTEM 21. ¿LA EMPRESA HA ESTABLECIDO POLÍTICAS O PROCEDIMIENTOS PARA ASEGURAR LA DISPONIBILIDAD DE LA INFORMACIÓN?	33
TABLA 31. ÍTEM 22. ¿LA EMPRESA HA ESTABLECIDO POLÍTICAS O PROCEDIMIENTOS PARA VERIFICAR LA AUTENTICIDAD DE LA INFORMACIÓN?.....	34
TABLA 32. ÍTEM 23. ¿LA EMPRESA HA ESTABLECIDO POLÍTICAS O PROCEDIMIENTOS PARA VERIFICAR LA TRAZABILIDAD DE LA INFORMACIÓN?	35
TABLA 33. ÍTEM 24. ¿EXISTE ALGÚN PROCEDIMIENTO PARA RESOLVER SITUACIONES INESPERADAS DE PÉRDIDA DE INFORMACIÓN?	36
TABLA 34. ÍTEM 25. ¿SE LLEVAN A CABO RESPALDOS DE LA INFORMACIÓN DE LA EMPRESA COMO ESTRATEGIA DE RESGUARDO Y ASEGURAMIENTO DE LA INFORMACIÓN?	37
TABLA 35. RESULTADOS DE VARIABLE DEPENDIENTE POR CADA UNA DE SUS DIMENSIONES Y SUS INDICADORES EN BASE AL INSTRUMENTO APLICADO.....	39
TABLA 36. RESULTADOS DE VARIABLE INDEPENDIENTE POR CADA UNA DE SUS DIMENSIONES Y SUS INDICADORES EN BASE AL INSTRUMENTO APLICADO.....	39
TABLA 37. PRUEBA DE NORMALIDAD.....	40
TABLA 38. INTERPRETACIÓN DEL COEFICIENTE DE CORRELACIÓN RHO DE SPEARMAN	41
TABLA 39. CORRELACIÓN ENTRE LAS VARIABLES DE LA HIPÓTESIS GENERAL	42
TABLA 40. RESUMEN DEL MODELO – REGRESIÓN LINEAL Y R ² (METODOLOGÍA MAGERIT V3, SEGURIDAD DE LA INFORMACIÓN).....	42
TABLA 41. PRUEBA DE ANOVA, INDEPENDIENTE Y DEPENDIENTE	43
TABLA 42. CRITERIOS DE VALORACIÓN DE ACTIVOS.....	52
TABLA 43. DIMENSIONES DE LA VALORACIÓN DE ACTIVOS	53
TABLA 44. IDENTIFICACIÓN DE AMENAZAS	55
TABLA 45. PROBABILIDAD DE OCURRENCIA.....	57
TABLA 46. DEGRADACIÓN DEL ACTIVO	57
TABLA 47. ASPECTO DE LAS SALVAGUARDAS.....	59
TABLA 48. TIPO DE PROTECCIÓN.....	59
TABLA 49. PESOS RELATIVOS	60
TABLA 50. NIVEL DE MADUREZ.....	60
TABLA 51. CALIFICACIÓN DE LOS RIESGOS	72
TABLA 52. SISTEMA DE GESTIÓN SISGECO	74
TABLA 53. SOFTWARE SISCONT.....	76
TABLA 54. SOFTWARE START SOFT PLANILLAS	77
TABLA 55. SISTEMA DE GESTIÓN DE BASE DE DATOS	79
TABLA 56. SISTEMA INTRANET	81
TABLA 57. SERVIDOR DE BASE DE DATOS.....	83
TABLA 58. SERVIDOR DE APLICACIONES	84
TABLA 59. CENTRAL IP	85
TABLA 60. RED LAN.....	86

TABLA 61. COMPUTADORAS DE ESCRITORIO	87
TABLA 62. CALENDARIZACIÓN DE HITOS PARA TRATAR LOS PRINCIPALES RIESGOS...	96
TABLA 63. FINANCIAMIENTO DE MEDIDAS PARA TRATAR LOS PRINCIPALES RIESGOS..	98
TABLA 64. OPERACIONALIZACIÓN DE LA VARIABLE INDEPENDIENTE METODOLOGÍA MAGERIT V3.....	111
TABLA 65. TABLA DE OPERACIONALIZACIÓN DE LA VARIABLE DEPENDIENTE SEGURIDAD DE LA INFORMACIÓN DE LA EMPRESA DECO INTERIORS	112
TABLA 66. IDENTIFICACIÓN DE ACTIVOS	149
TABLA 67. VALORACIÓN DE ACTIVOS	150
TABLA 68. IDENTIFICACIÓN DE AMENAZAS	151
TABLA 69. VALORACIÓN DE AMENAZAS	168
TABLA 70. IDENTIFICACIÓN Y VALORACIÓN DE LAS SALVAGUARDAS	186
TABLA 71. RIESGO POTENCIAL DE LOS ACTIVOS.....	187
TABLA 72. RIESGO RESIDUAL DE LOS ACTIVOS.....	189
TABLA 73. IMPACTO POTENCIAL SOBRE CADA UNO DE LOS ACTIVOS	191
TABLA 74. IMPACTO RESIDUAL ACUMULADO	193

FIGURA

FIGURA 1. FASES PARA EL ANÁLISIS DE LOS RIESGOS.....	23
FIGURA 2. ELEMENTOS DEL ANÁLISIS DE RIESGOS POTENCIALES	25
FIGURA 3. ÍTEM 1. ¿LA EMPRESA LE HA PROPORCIONADO CAPACITACIÓN SOBRE EL RESGUARDO DE LA INFORMACIÓN QUE ADMINISTRA?.....	13
FIGURA 4. ÍTEM 2. ¿LA EMPRESA LE HA PROPORCIONADO INFORMACIÓN SOBRE LOS RIESGOS TECNOLÓGICOS DE LA INFORMACIÓN QUE ADMINISTRA?.....	14
FIGURA 5. ÍTEM 3. ¿PONE EN PRÁCTICA ALGUNA ESTRATEGIA PARA LA PROTECCIÓN DE LA INFORMACIÓN?.....	15
FIGURA 6. ÍTEM 4. ¿LA EMPRESA HA IMPLEMENTADO ALGUNA ESTRATEGIA PARA CONCIENTIZAR AL PERSONAL SOBRE LOS RIESGOS E IMPORTANCIA DE LOS ACTIVOS DE INFORMACIÓN?.....	16
FIGURA 7. ÍTEM 5. ¿SE CONSIDERA COMPROMETIDO CON EL RESGUARDO DE LA INFORMACIÓN QUE ADMINISTRA?	17
FIGURA 8. ÍTEM 6. ¿LA EMPRESA HA IMPLEMENTADO ALGUNA ESTRATEGIA PARA EVALUAR LOS RIESGOS A LOS QUE ESTÁ SOMETIDA LA INFORMACIÓN?	18
FIGURA 9. ÍTEM 7. ¿LA EMPRESA HA DETERMINADO LOS RIESGOS A LOS QUE ESTÁN SOMETIDOS LOS ACTIVOS DE INFORMACIÓN?.....	19
FIGURA 10. ÍTEM 8. ¿LA EMPRESA HA IDENTIFICADO LOS RIESGOS SOBRE LA INFORMACIÓN QUE AFECTARÍAN LAS LABORES DIARIAS?	20
FIGURA 11. ÍTEM 9. ¿SE HAN CUANTIFICADO EN LA EMPRESA LOS POSIBLES DAÑOS EN LOS ACTIVOS DE INFORMACIÓN?	21
FIGURA 12. ÍTEM 10. ¿LA TECNOLOGÍA DE INFORMACIÓN DISPONIBLE EN LA EMPRESA ES ADECUADA PARA EL DESARROLLO DE LAS ACTIVIDADES?	22
FIGURA 13. ÍTEM 11. ¿LA TECNOLOGÍA DE INFORMACIÓN DISPONIBLE EN LA EMPRESA GARANTIZA LA SEGURIDAD DE LA INFORMACIÓN?	23
FIGURA 14. ÍTEM 12. ¿EL SERVICIO DE INTERNET DISPONIBLE EN LA EMPRESA ES ADECUADO PARA LLEVAR A CABO SUS ACTIVIDADES?.....	24
FIGURA 15. ÍTEM 13. ¿LAS COMPUTADORAS ESTÁN CONECTADAS CON LA RED PARA ENVIAR Y RECIBIR INFORMACIÓN?	25
FIGURA 16. ÍTEM 14. ¿SU NIVEL DE PERICIA LE PERMITE REALIZAR UN ADECUADO ASEGURAMIENTO DE LA INFORMACIÓN QUE ADMINISTRA?	26
FIGURA 17. ÍTEM 15. ¿REQUIERE DE ALGÚN TIPO DE ASISTENCIA PARA RESOLVER PROBLEMAS INFORMÁTICOS DURANTE SUS LABORES DIARIAS?.....	27
FIGURA 18. ÍTEM 16. ¿EL SERVICIO DE INTERNET LE PERMITE INGRESAR A TODAS LAS PÁGINAS WEB QUE DESEE?	28
FIGURA 19. ÍTEM 17. ¿PUEDE RECIBIR Y ENVIAR CORREOS DESDE SU COMPUTADORA DE TRABAJO?.....	29
FIGURA 20. ÍTEM 18. ¿CONSIDERA QUE SU NIVEL DE CONOCIMIENTO EN EL MANEJO DE LA TECNOLOGÍA INFORMÁTICA ES SÓLIDO?.....	30
FIGURA 21. ÍTEM 19. ¿LA EMPRESA HA ESTABLECIDO POLÍTICAS O PROCEDIMIENTOS PARA ASEGURAR LA CONFIDENCIALIDAD DE LA INFORMACIÓN?	31
FIGURA 22. ÍTEM 20. ¿LA EMPRESA HA ESTABLECIDO POLÍTICAS O PROCEDIMIENTOS PARA ASEGURAR LA INTEGRIDAD DE LA INFORMACIÓN?	32
FIGURA 23. ÍTEM 21. ¿LA EMPRESA HA ESTABLECIDO POLÍTICAS O PROCEDIMIENTOS PARA ASEGURAR LA DISPONIBILIDAD DE LA INFORMACIÓN?	33

FIGURA 24. ÍTEM 22. ¿LA EMPRESA HA ESTABLECIDO POLÍTICAS O PROCEDIMIENTOS PARA VERIFICAR LA AUTENTICIDAD DE LA INFORMACIÓN?.....	34
FIGURA 25. ÍTEM 23. ¿LA EMPRESA HA ESTABLECIDO POLÍTICAS O PROCEDIMIENTOS PARA VERIFICAR LA TRAZABILIDAD DE LA INFORMACIÓN?	35
FIGURA 26. ÍTEM 24. ¿EXISTE ALGÚN PROCEDIMIENTO PARA RESOLVER SITUACIONES INESPERADAS DE PÉRDIDA DE INFORMACIÓN?	36
FIGURA 27. ÍTEM 25. ¿SE LLEVAN A CABO RESPALDOS DE LA INFORMACIÓN DE LA EMPRESA COMO ESTRATEGIA DE RESGUARDO Y ASEGURAMIENTO DE LA INFORMACIÓN?	37
FIGURA 28. DATOS DEL PROYECTO.....	47
FIGURA 29. IDENTIFICACIÓN DE ACTIVOS.....	49
FIGURA 30. DEPENDENCIA ENTRE ACTIVOS	51
FIGURA 31. VALORACIÓN PROPIA DE LOS ACTIVOS.....	54
FIGURA 32. IDENTIFICACIÓN DE AMENAZAS EN CADA UNO DE LOS ACTIVOS	56
FIGURA 33. VALORACIÓN DE LAS AMENAZAS SOBRE LOS ACTIVOS	58
FIGURA 34. IDENTIFICACIÓN Y VALORACIÓN DE LAS SALVAGUARDAS	61
FIGURA 35. RIESGO POTENCIAL DE LOS ACTIVOS	63
FIGURA 36. RIESGO RESIDUAL DE LOS ACTIVOS.....	65
FIGURA 37. IDENTIFICACIÓN DE RIESGOS POR ACTIVOS	66
FIGURA 38. IMPACTO POTENCIAL SOBRE CADA UNO DE LOS ACTIVOS	68
FIGURA 39. IMPACTO RESIDUAL	69
FIGURA 40. RIESGO POTENCIAL Y RIESGO RESIDUAL SOBRE LOS PRINCIPIOS DE LA SEGURIDAD	70
FIGURA 41. RIESGO POTENCIAL VS RIESGO RESIDUAL EN CADA UNO DE LOS PRINCIPIOS DE LA SEGURIDAD.....	71
FIGURA 42. IDENTIFICACIÓN DE RIESGOS CRÍTICOS	73

RESUMEN

En esta investigación se planteó la finalidad de definir la influencia de la Metodología Magerit V3 en la seguridad de la información de la empresa Deco Interiors SAC, para lo cual se estableció el siguiente planteamiento metodológico: investigación de tipo aplicada con un diseño correlacional descriptivo, en una población de 115 colaboradores de donde se obtuvo una muestra correspondiente a los responsables del departamento de informática a los cuales se les aplicó un instrumento realizado y validado por juicio de expertos. Al procesarse e interpretarse los resultados conseguidos pudo evidenciarse una correlación positiva importante de 0.781 de la Metodología Magerit V3 y la seguridad de la información con un nivel de significancia por debajo de 0.05 propuesta en la investigación, así mismo, se determinó que la seguridad de la información se encuentra explicada en un 70.6% por la Metodología Magerit V3 realizada en la empresa. De esta manera, se confirma que hay influencia significativamente de una variable sobre la otra, lo que le asegura a la empresa la necesidad de aplicar la Metodología Magerit para poner en práctica una apropiada gestión de los riesgos a los que se encuentran expuestos sus activos de información.

Palabras Clave: Metodología Magerit, seguridad de la información, gestión de riesgo.

ABSTRACT

The purpose of this research was to define the influence of the Magerit V3 Methodology on the information security of the company Deco Interiors SAC, for which the following methodological approach was established: applied research with a descriptive correlational design, in a population of 115 collaborators from which a sample corresponding to the heads of the IT department was obtained to whom an instrument made and validated by expert judgment was applied. When processing and interpreting the results obtained, an important positive correlation of 0.781 of the Magerit V3 Methodology and the security of the information with a level of significance below 0.05 proposed in the research could be evidenced, likewise, it was determined that the security of the 70.6% of the information is explained by the Magerit V3 Methodology carried out in the company. Thus, it is confirmed that there is significant influence of one variable on the other, which assures the company of the need to apply the Magerit Methodology to implement an appropriate management of the risks to which its information assets are exposed.

Keywords: Magerit methodology, information security, risk management.

I. INTRODUCCIÓN

1.1. Planteamiento del problema.

La tecnología de la información y las comunicaciones (TIC) viene siendo adoptada ampliamente por los procedimientos y actividades de las organizaciones modernas. La dependencia de las TIC se ha convertido en un reto continuo para los expertos e investigadores en materia de seguridad, ya que su protección es vital debido a las numerosas amenazas a las que están expuestas. Cuando se trata de la seguridad de la información, las compañías tienen el objetivo de mantener la confidencialidad, disponibilidad, integridad, responsabilidad, legitimidad y fiabilidad de los sistemas informáticos y sus datos (Schumacher et al., 2013). Además, toda organización se enfrenta a amenazas que podrían obstaculizar sus actividades, crecimiento y rentabilidad (Espinoza 2019). Estas amenazas aumentan el factor de riesgo del sistema de las TIC y dan lugar a la aparición de varias exigencias de seguridad, que deben satisfacerse de forma adecuada y sistemática para garantizar la protección del sistema.

El medio para elaborar una estrategia y una hoja de ruta de seguridad es la estimación del riesgo, al cual se enfrenta la organización, además facilita la estimación y el cálculo de los mismos. El riesgo se representa principalmente en función del grado de daño y la posibilidad de que ocurra un daño (NIST 2012). La gestión del riesgo tiene por objeto identificar, controlar y atenuar los riesgos para los sistemas de información (Nieves 2017). Así pues, la evaluación de los riesgos es una piedra angular de la gestión de los riesgos, que incluye pasos que pueden agruparse en las cuatro fases siguientes: i) determinación del riesgo afrontado, ii) evaluación del riesgo, iii) medidas de respuesta para mitigar el riesgo, y iv) vigilancia del riesgo (NIST, 2012).

Existen muchas metodologías para realizar un diagnóstico de los riesgos, pero se necesita de un modelo de activos de la empresa. Generalmente dentro del modelo se incluye los valores de los activos,

sobre todo de los más importantes para la empresa, además de sus dependencias. Identificar los activos y su valoración es el primer paso de cualquier procedimiento de evaluación de riesgos. El segundo paso es organizar los activos en capas y la implantación de dependencias de los activos de distintas capas e incluso entre la misma capa. Por último, se genera un diagrama de dependencia de todos los activos. Debe de desarrollarse este proceso en cada una de las dimensiones de la seguridad: confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad (Fernández y García, 2016).

En vista que en la actualidad se dispone de diversos métodos heterogéneos de evaluación de riesgo, cada uno con un enfoque diferente, los analistas tienen que elegir el que mejor se adapte a la organización que será evaluada. Aunado a la heterogeneidad de los métodos, en la actualidad no hay consenso con respecto a este proceso de selección (Fernández y García, 2016).

Tomando en cuenta las necesidades manifiestas de la empresa Deco Interiors SAC, en las que solicita incluir en sus procesos prácticas enfocadas al resguardo de la información; motivo por el cual se precisa llevar a cabo una evaluación del riesgo al que se encuentran sometidos los activos y saber cuáles son las diferentes formas o mecanismos que permiten disminuir las amenazas lleguen a convertirse en realidad.

A partir de ello se estableció que el método más conveniente para atenderlas, sobre la base de las especificaciones técnicas, operacionales y de procedimiento de los métodos, es la Metodología Magerit. Esta metodología cumple muy bien con este requisito, además, aporta un método abreviado de la valoración de los activos que disminuye considerablemente en trabajo de modelación (Amutio y Mañas, 2014). Con base en ello, se presentará a la empresa la influencia de dicha metodología en los procesos de seguridad de su información.

1.2. Antecedentes de estudio

En el ámbito internacional.

Molina-Miranda (2017) en su investigación sobre análisis de riesgos de centro de datos dirigida a establecer los primordiales riesgos que están sometidos los activos mediante la aplicación de metodología MAGERIT, expuso que el referido análisis consintió reconocer el grado de madurez en la seguridad que se aplica en la corporación sobre las cuales se sugirieron las protecciones para minimizar los niveles de riesgo e impacto. Agregó que la gestión de los riesgos en cualquier organización debe valorarse como un proceso intrínseco, lo que le permitirá definir las estrategias para evitar una posible ocurrencia. De acuerdo a los resultados conseguidos la entidad reconoció que necesita poner en marcha un proyecto de gestión de riesgos que consienta aminorar los más críticos y luego avanzar hacia el despliegue de un plan de tratamiento de riesgo.

Imbaquingo et al., (2019) en su estudio sobre evaluación de sistemas de seguridad informáticos universitarios dirigida a crear objetivos y controles que consientan disminuir las vulnerabilidades del sistema de gestión, señalaron que el elemento que acrecienta el nivel de los riesgos del activo de información es el insuficiente procedimiento aplicado para evitar dichas situaciones, es decir, no hay una cultura de riesgos posibles que consigan perturbar la disponibilidad, confidencialidad e integridad de la información con la cual se trabaja. Una vez que se logra determinar la situación actual del sistema esgrimiendo la metodología MAGERIT, se evidenció un grado de acatamiento de políticas de seguridad de información de 51%, bien físicas como de gestión, derivando en que es necesario que las autoridades y docentes se comprometan para que la normativa logre cumplirse en su totalidad.

Viteri, Cano, Zambrano y Minaya (2019) en su estudio para evaluar las incidencias, riesgos y vulnerabilidades presentes en la infraestructura tecnológica de una institución universitaria, dirigida a presentar un

Modelo de Gestión de Continuidad que evalúe de manera continua los riesgos de los activos de información, analice el impacto en los negocios y presente estrategias de recuperación. Los resultados del estudio expusieron que el total de los activos de información está sometido a 59% de riesgos críticos causados por amenazas con un nivel alto de criticidad, y que al aplicar el modelo propuesto la institución puede responder de forma significativa ante posibles incidentes permitiendo dar continuidad a las operaciones en beneficios de la comunidad universitaria.

Crespo (2016) en su estudio sobre la gestión del riesgo informático en Mpymes se enfocó en el desarrollo de una metodología para la seguridad de la información enmarcadas dentro de la referencia de las normas ISO, debido a la ausencia de esta y de un plan de contingencia para recuperación en caso de ser necesario. A partir de los resultados alcanzados resaltó la importancia de la metodología Magerit V3 en el proceso de gestión de riesgos sobre la cual los entes gubernamentales pueden tomar decisiones valorando los riesgos procedentes al emplear las TI. Agregó que el periodo de tratamiento de riesgos en las organizaciones comprende a procedimientos en cuanto a seguridad para subsanar las exigencias reveladas por el análisis, y comprende cuatro fases constantes: Planificación, implementación y operación, monitorización y evaluación, mantenimiento y mejora, las cuales deben ser implementadas de forma continua para disminuir los riesgos en los activos de información.

En el ámbito nacional.

Briceño (2019) enfocó su estudio en la realización de un plan para mejorar la protección de los activos en una zona económica en desarrollo (ZED) considerando la importancia de la información de dicha zona. El análisis arrojó que la ZED presenta medidas de seguridad en una etapa inicial inadecuadamente aprovechadas y que la utilización de la metodología MAGERIT consiente ejecutar un estudio de los riesgos valorando los activos, las amenazas y salvaguardas actuales sobre las

que se pueden implementar futuras protecciones para controlar y aminorar los riesgos hallados. Añadió que otra ventaja de la utilización de la metodología MAGERIT es que permite reconocer el impacto que crearía si la amenaza se materializa, agregando gráficas que contrastan los impactos existentes. A esto se suma que el procedimiento para optimizar la seguridad de la información se realiza bajo las normas ISO que resultan obligatorias en todas las instituciones del estado.

Jara (2018) en su investigación acerca de la influencia del SGSI sobre la gestión del riesgo y sí existe una influencia significativa, la cual fue determinada con evidencias estadísticas, además la implementación de dicho sistema influye en el tratamiento de la gestión del riesgo corroborado a través del procedimiento de Wilcoxon, donde la comparación de ambos grupos, se evaluó a través de dicho procedimiento, siendo ésta significativa.

Ayala (2017) acerca de su investigación sobre SGSI y la mejora del proceso de gestión del riesgo, se enfocó en determinar la disminución del riesgo al que se ven expuestos los activos de información. Los resultados evidenciaron que implementar esta metodología logra disminuir el nivel del riesgo un 16.96%, generando así una disminución de los controles no existentes en 72.38% y por consiguiente, el aumento de los controles que existen en 76.19%; respecto a los controles en parte llevados a cabo se reducen en 3.81. A nivel general, implementar una metodología del SGSI logra optimizar el proceso de gestión del riesgo de los activos.

Tarrillo (2016) de una forma similar, su estudio realizado corroboró la influencia de la gestión del riesgo sobre la seguridad de los activos soportado en los resultados estadísticos, demostrando que existe relación entre las variables. A su vez presentó el “alto” nivel de riesgo de los activos de información medido en un 52%, como resultado del análisis de las dimensiones evaluadas. Adicionalmente, el estudio arrojó que los factores de riesgo que afectan a los activos de información son

“altos” y representan un 54% soportado también en el análisis de las dimensiones evaluadas.

En el ámbito local.

Ñañez (2019) enfocó su investigación para diseñar un modelo de gestión de riesgos con base en el estándar ISO/IEC 27005 cuyo propósito fue mejorar la gestión de seguridad de la información a través de la metodología de MAGERIT. El desarrollo del estudio permitió su cometido y desarrolló un procedimiento para identificar los procesos críticos que permitieron la evaluación de los escenarios de riesgos de la organización, añadió que el procedimiento elaborado permite desplegar las labores y trabajos de las primordiales etapas de un sistema de gestión de riesgos que son: evaluar y tratar los riesgos; teniendo en cuenta los activos de la empresa. Otra importancia resaltada del modelo propuesto es que admite, con coherencia, claridad y capacidad para todo activo de TI, apreciar su criticidad, ubicar las amenazas y debilidades que componen los espacios de riesgos y por último valorar las diferentes circunstancias de exposición al riesgo, fundamentado en un estudio de los impactos y periodicidades de ocurrencia de los contextos de riesgo establecidos.

León (2019) basó su estudio en el desarrollo de un modelo basado en metodologías de gestión de riesgos para mejorar la seguridad de los activos de información en empresas del sector agroindustrial. Alcanzó su objetivo y propuso un modelo para gestionar el riesgo de IT para ayudar en el progreso de la seguridad de los activos cuya validación se logró con su implementación en una de las empresas, el cual permitió identificar 20 escenarios de riesgo, de los cuales 13 eran especificados como inadmisibles y 7 como tolerables. Para las situaciones en la que los niveles de riesgo no se consideraban aceptables para la compañía, se plantearon 8 planes que consentirían reducir el nivel de riesgo presente.

Puyén y Rivas (2018) Requerían incrementar la gestión de seguridad de la información en una institución de la región, por lo que se enfocaron en implementar un diseño para gestionar los riesgos considerando como marco de referencia la norma ISO/IEC 27005 y metodología Magerit. Los resultados analizados indicaron que la institución no tiene reglas, estrategias o alguna maniobra para manejar la seguridad de la información por lo que la utilización del modelo formulado consentiría dar cumplimiento a 6 de los 8 directrices determinadas en la política de seguridad de la información estipulado por el Ministerio, destacando de esa manera la importancia del estudio para la organización. Resaltaron que el modelo exhibido cuenta con un moderado - alto nivel de suficiencia, claridad, coherencia y relevancia, volviéndolo una guía válida para ejecutar la gestión de riesgos y de provecho para la institución.

Santa Cruz (2016) basó su investigación en implementar una metodología de gestión de riesgos de información que le permitiera a una organización obtener una certificación ISO 27001, permitiéndole a la vez reducir los riesgos de los activos de información. La herramienta obtenida con el desarrollo del estudio fue capaz de determinar y enfrentar los riesgos y hacerle seguimiento, dando cumplimiento a la estructura del método llevado a cabo y la aprobación de los directivos del organismo. Esto permitiría estimar lo que podrá suceder, así como también permite el análisis de dichos aspectos de manera ordenada, obteniendo conclusiones con base y conseguir resultados positivos que certifiquen la continuación del negocio. A partir de dicha metodología la institución puede establecer la defensa minuciosa y prudente, previniendo acontecimientos dañinos y simultáneamente encontrarse capacitados para detener las posibles incidencias, mantenerse luego de los accidentes y continuar trabajando en óptimas condiciones. Añadió finalmente que, su aplicación reduce el riesgo a un nivel residual que puede ser asumida por la institución y que bajo estas condiciones podrá conseguir la Certificación ISO 27001, y de esta manera lograr mayor reputación de la que ya posee.

1.3. Abordaje teórico (Marco Teórico)

1.3.1. Teorías relacionadas al tema.

Metodología para el análisis y la gestión de riesgos de los sistemas de información (MAGERIT)

Es utilizada como método común para el marco de gestión de riesgos según los estándares ISO/CEI 27001. Esta metodología es sencilla y rápida de aplicar, proporciona buenos resultados sobre el estado del riesgo y puede utilizarse como base de apoyo al tomar decisiones para la mejora (Fernández y García, 2016).

La metodología MAGERIT estipula los valores de los activos tomando en cuenta aspectos como la disponibilidad, integridad, confidencialidad, trazabilidad y autenticidad, instituyendo distintos grados de apreciación, como: muy alto, alto, medio, bajo, muy bajo y despreciable, en dicho método es comprobado el impacto estableciendo el valor de los activos, dicho acumulado es calculado por medio del valor del activo y las amenazas a las que se enfrenta, y dicha afectación resulta es tomada como el valor propio y las amenazas (Amutio et al, 2012). Según estos autores la metodología en estudio se fundamenta en los conceptos siguientes:

Activos: Es todo aquello que puede ser valioso para una empresa, el cual podría ser material o intangible. Éstos tienen que ser identificados y valorados, aunque, MAGERIT indica que el criterio para evaluar los activos no tiene que ser el valor real, sino el valor estimado de los daños causados en la empresa por el mal funcionamiento de una o más dimensiones de seguridad.

Dependencias: Así como los activos, tenemos que establecer las dependencias que existen entre ellos, de esta manera podemos identificar como se propaga el impacto y el riesgo entre un activo y otro. MAGERIT propone que los activos principales (información), tienen que colocarse en el nivel superior del gráfico de las dependencias, luego los

servicios, y en un nivel inferior los activos como el hardware, el software y las comunicaciones. En cada una de las dependencias se tiene que mencionar las dimensiones de seguridad comprometidas y el porcentaje de dependencia.

Amenazas: Las amenazas deben ser identificadas para cada activo, en cada dimensión y evaluarse según su frecuencia y la degradación que provoca en el activo si se materializa. MAGERIT nos facilita las amenazas relacionadas con cada activo. Para que la correcta identificación y asignación de clases a los activos sea esencial para empezar. Además, puede ser necesario añadir amenazas específicas según sea apropiado. Molina (2015) refiere que las amenazas vienen a ser debilidades o fragilidades de un activo que pudiesen explotarse por uno o más orígenes potenciales de una eventualidad, que consigue repercutir en posibles daños a los activos y en consecuencia a la empresa; las amenazas son aspectos que consiguen perjudicar o afectar la información de una u otra manera, las mismas por lo general pueden encontrarse comenzando en una debilidad presente. Así mismo, se clasifican en diferentes tipos: de origen natural, del entorno, por defecto de aplicaciones, producidas por individuos a causa de un accidente o de manera intencional.

Salvavidas: Al igual que en las amenazas, MAGERIT facilita una gran lista de salvavidas las cuales están asociadas a los activos y las amenazas. De esta forma, podemos usar un listado para verificar y establecer cuáles serán aplicadas y su madurez.

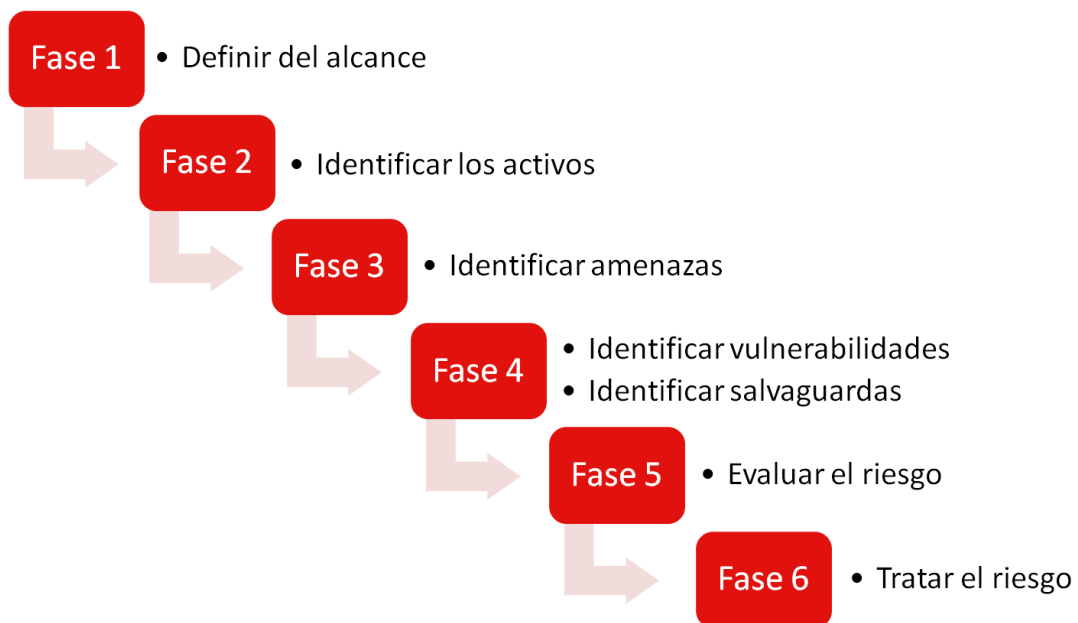
Esto va a depender de las características en particular de cada empresa y de ser necesario se pueden aplicar salvavidas personalizadas según sea el caso.

Según el Libro I de MAGERIT, el primer paso es el reconocimiento de los activos y clasificarlos en grupos proporcionada por la herramienta EAR PILAR, esta aplicación nos ayuda a utilizar la metodología MAGERIT. A continuación, es imprescindible formar el árbol de

dependencias entre todos los activos previamente definidos. Finalmente, cuando estén relacionados y definidos los activos necesitaremos asignarle un valor a cada uno de ellos. Cuando estén bien descritos los activos, MAGERIT determinara las potenciales amenazas y, usando su valoración de impacto, podremos determinar el riesgo (Amutio, et al, 2012).

Figura 1.

Fases para el análisis de los riesgos.



Nota. Fases de las metodologías para el análisis de riesgos. Tomado de (INCIBE, 2017)

MAGERIT permite realizar la evaluación de riesgos a través de:

- Identificación de riesgos: Realiza el reconocimiento de los activos, las relaciones entre ellos, la valoración para la empresa, la identificación de las amenazas y la evaluación de los riesgos. Los conocimientos importados provienen del conocimiento del entorno del sistema, de los informes de decisiones similares de las estadísticas cuando procede. La disponibilidad de los datos queda mejor ilustrada por la representación en la información cuantitativa.

La aportación de datos para el análisis cualitativo consiste en determinar los escenarios y para el análisis cuantitativo son las categorías de las escalas y los datos de los costos. Tiene la capacidad de convertir los datos cuantitativos, para ser adoptados o representados en datos cualitativos utilizando escalas aproximadas. Los datos que se tienen en cuenta para la valoración son la confidencialidad, la integridad, la disponibilidad, la autenticidad y la responsabilidad de imputación.

- Análisis de riesgos: Calcula el impacto y el riesgo, los valores posibles y los restantes. Cuantitativo y cualitativo, acumulado y desviado. Realiza un análisis de riesgo básico. La definición del riesgo se basa en tres parámetros: escenario de la amenaza, posibilidad y consistencia (multidimensional, típicamente medible usando escalas de categorías). La probabilidad está relacionada con un período de medición que suele ser el tiempo de duración de las inversiones (40 años). La metodología recibe datos cualitativos y cuantitativos.

Figura 2.

Elementos del análisis de riesgos potenciales



Nota. Tomado de Magerit, Libro I, Pág. 17 (Públicas, 2012).

- Evaluación del riesgo: Prioriza los resultados y éstos se presentan a los administradores para la evaluación operacional. El método básico de análisis de riesgos se apoya en la creación de escenarios (en la práctica "basados en hechos") y en la evaluación de las consecuencias y probabilidades (frecuencias) relacionadas con los escenarios. Las escalas de consecuencias suelen estar clasificadas por categorías.

En síntesis, MAGERIT permite identificar, analizar y evaluar las alternativas propuestas de acuerdo con la cantidad de reducción alcanzada (o riesgo residual). El riesgo se determina en función de las posibles cantidades de pérdida, y se correlaciona con las posibles pérdidas con probabilidades específicas. El resultado del análisis de riesgos proporciona valores modelo de las dependencias entre los diversos componentes y la cantidad de amenazas a las que están expuestos los elementos. También evalúa la eficacia de las medidas existentes. Por último, hace una clasificación de las medidas para el riesgo. Plan de seguridad - Programas de seguridad total que implementan las decisiones para la gestión de riesgos (Motaki, 2016).

El método Magerit es una metodología general que permite realizar análisis cualitativos y cuantitativos. La evaluación del impacto se basa en los activos críticos, la evaluación del riesgo tiene en cuenta la probabilidad, la vulnerabilidad (activo crítico) y el impacto (amenaza, activo) (Motaki, 2016).

Seguridad de la Información

Las organizaciones utilizan la información que crean y procesan las personas y los sistemas en los procesos para lograr sus objetivos comerciales. Para una organización es fundamental proteger y asegurar esta información, que presenta un valor. En el pasado, la seguridad se asociaba principalmente a los datos y sistemas y no a la información. Sin embargo, con el tiempo, la comprensión de la seguridad cambió de una visión de los sistemas a una visión de la información en la informática (Taubenberger, 2014).

La seguridad de los datos se convirtió en seguridad informática, y la seguridad informática se convirtió en seguridad de la tecnología de la información (TI) y la seguridad de la TI se convirtió en seguridad de la información debido a la mejor comprensión del impacto comercial y el riesgo asociado de no proteger adecuadamente los recursos electrónicos de una empresa" (von Solms y von Solms, 2005).

La expresión "seguridad de los datos" evolucionó con el tiempo hasta convertirse en "seguridad de la información" debido a la mayor concordancia de los sistemas de información con las operaciones comerciales y los procesos de contabilidad financiera que requieren la protección de la información empresarial. Debido a la mayor concordancia entre los procesos comerciales y los sistemas informáticos, si alguno de los pilares de la seguridad de la información faltase, puede causar efectos adversos graves a una organización y a sus objetivos comerciales. Por lo tanto, la información necesita resguardarse siempre apropiadamente. La protección de la información, identificando las necesidades de seguridad,

así como los riesgos para la información, requiere que se establezcan procesos adecuados (Taubenberger, 2014).

Delgado (s/f) conceptualiza la seguridad de la información como un grupo de disposiciones protectoras y que buscan un resultado, de las empresas que consienten cuidar y preservar la información intentado conservar las dimensiones (confidencialidad, disponibilidad e integridad) de esta.

Shameli-Sendi, Aghababaei-Barzegar y Cheriet (2016) definen la seguridad de la información como un ligado de metodologías, labores y operaciones que pretenden resguardar la información como activo valioso, con la finalidad de disminuir la amenaza y el riesgo continuo al que se encuentra sometida, además de cerciorarse que el negocio pueda continuar, reducir los perjuicios a la empresa y extender el regreso de las inversiones y oportunidades de la organización.

Cano (2011) refiere la seguridad de la información como la disciplina que se refiere a los riesgos, de las amenazas, del estudio de escenarios, de las correctas prácticas y esquemas normativos, que demandan niveles de protección de procesos y tecnologías para enaltecer el grado de confianza en la creación, utilización, almacenamiento, transferencia, recobro y disposición final de la información.

Amutio et al (2012) expresan que la seguridad es la capacidad de los sistemas de información para hacer frente, con cierto grado de seguridad, los incidentes o prácticas indebidas que afecten las dimensiones de la seguridad de la información almacenada o transferida y de los servicios que los mismos brindan o permiten que sean asequibles.

ISO 27001 (2013) establece que la seguridad de la información radica en el resguardo de su integridad, confidencialidad y disponibilidad, de igual manera de los sistemas involucrados en su tratamiento, en el seno de una empresa.

Queda entendido por Seguridad de la Información, la totalidad de determinadas disposiciones preventivas y reactivas que se ejecutan en

las organizaciones para cuidar y preservar los datos pretendiendo conservar la confiabilidad, la legitimidad y probidad de esta.

Características de un Sistema de Información Seguro

Disponibilidad: Encontrarse disponible y aprovechable al momento de ser requerida por una institución autorizada se convierte en una de sus características. La información debe hallarse disponible para quienes deban tener acceso a la misma, estos pueden ser individuos, procedimientos o aplicaciones. Consiste en acceder a la información y a las redes, respecto al servicio por motivos de falta de electricidad, deficiencias de hardware y sistema con actualizaciones. Involucra asimismo la prevención de ataque de negativa de servicio (ISO 27001:2013).

Confidencialidad: La información se encuentre disponible y no logre divulgarse a individuos, instituciones o procedimientos no autorizados es otra particularidad. Acceder a la información exclusivamente individuos que tienen el requerido permiso (ISO 27001:2013).

Integridad: Rasgo que consiste en proteger la precisión y totalidad de los activos. Pretende conservar la información exenta de reformas no autorizadas, con el fin de guardarla así como se generó, sin ser manipulada ni cambiada por individuos o procedimientos no autorizados (ISO 27001:2013).

Autenticidad: Certeza de que un mensaje, una transacción o distintos intercambios de información procede de la fuente de la que asevera ser. Autenticidad involucra prueba de identidad (ISO 27001:2013). La misma consigue comprobarse mediante una autenticación. Dicho proceso comúnmente incluye más de una "prueba" de identidad (no obstante una es suficiente).

Trazabilidad: Es la ratificación de que en cualquier instante o tiempo se conseguirá establecer qué fue lo hecho por alguna persona y cuando se realizó. La trazabilidad es fundamental para examinar las eventualidades,

rastrear al agresor y tomar en cuenta lo sucedido como un aprendizaje; ésta puede materializarse en la integridad de los logs de actividad (ISO 27001:2013).

Riesgo

El análisis de riesgos se conoce como el procedimiento metódico en el que se mide el alcance de los peligros ante los cuales se encuentra una empresa y consiente establecer la naturaleza, el costo y la garantía que posee un sistema. (Amutio et al (2012).

Gestión de Riesgos

La totalidad de las empresas afrontan peligros de alguna clase regularmente (Calder y Watkins, 2008). Este tipo de gestión se caracteriza por ser una disciplina existente para manejar distintos peligros no especulativos, los cuales representan esos peligros de los cuales se desprende una pérdida para la empresa (Calder y Watkins, 2008). Igualmente, esta gestión acostumbra poseer los subsiguientes propósitos: prescindir de los peligros, disminuir escalas tales como "adecuados" esos riesgos imposibles de descartar y así vivir con ellos, en otras palabras, aceptarlos mediante la práctica de controles que los conserven cautelosamente en niveles "satisfactorios" o luego moverlos nuevamente, a través de planes de respaldo, por ejemplo, a una asociación diferente.

Elementos de riesgo.

Activos de Información: Aluden a cualquier elemento que posea datos. De acuerdo a la norma, los activos de información tendrían que encontrarse ordenados por la sensibilidad y la criticidad de los datos que contienen o según lo indicado por la utilidad que tienen y rotulados según sea necesario, para mostrar cómo deben tratarse y protegerse dichos datos. (Delgado, s/f).

Amenazas: Representan debilidades de un activo que puede ser explotadas por al menos uno de los posibles motivos de un accidente que puede causar daños a los activos y, por lo tanto, a la asociación; las amenazas son datos en alguna estructura, se pueden encontrar en su mayor parte a partir de una debilidad actual. Los peligros acostumbran organizarse en diversas clases, las cuales pueden originarse de manera natural, industrial, imperfección de la aplicación, provocada por individuos de manera consiente o intencional (Molina, 2015).

Vulnerabilidades: Los activos pueden verse afectados por una progresión de amenazas; la posibilidad de que aparezca alguna de ellas y la degeneración que conlleva un activo es reconocido como

vulnerabilidad acorde al método MAGERIT (Amutio et al 2012). Las vulnerabilidades tienen que enunciarse en una escala numérica y luego de esta manera evaluar su efecto, se recomienda que sean distinguidas y estimadas de manera individual (Crespo, 2016).

Impacto: Este indica lo que puede ocurrir al momento de aparecer las amenazas, viniendo a ser la proporción del perjuicio provocado por una amenaza cuando aparece en un activo (Molina, 2015).

1.3.2. Marco Conceptual.

- **Confidencialidad:** Implica la gravedad de que los datos sean conocidos por individuos ajenos o no facultados para ello (Taubenberger, 2014).
- **Integridad:** Es la importancia de que los datos no estén corruptos por una alteración malintencionada, involuntaria o estar incompletos (Taubenberger, 2014).
- **Disponibilidad:** Los datos deben estar accesibles para las personas autorizadas y a las consecuencias de no estar disponibles. (Taubenberger, 2014).
- **Autenticidad:** Rasgo o particularidad que consta en que una institución es la que dice ser o bien que avala la fuente de la cual provienen los datos (Amutio et al (2012).
- **Trazabilidad del uso del servicio:** Seguridad de que en cualquier instante se conseguirá establecer quién hizo qué y en qué momento (Amutio et al (2012).
- **Riesgo potencial:** Cualquier amenaza que incida en los pilares de la seguridad de la información en la integridad, disponibilidad y la confidencialidad son un riesgo para las empresas (Taubenberger, 2014).
- **Salvaguardas:** Se define como el procedimiento que reduce la acción o efecto que produce un riesgo o una amenaza (Amutio et al (2012).

- **Riesgo:** Es el indicador del nivel de presentación en el que aparece un peligro en al menos uno de los activos perjudicando a la organización, es decir, es lo que probablemente ocurra. (Molina, 2015).

1.4. Formulación del Problema.

1.4.1. Problema General

¿Cómo contribuir a la Seguridad de la Información de la Empresa Deco Interiors SAC?

1.5. Justificación e importancia del estudio.

La relevancia expuesta previamente acerca de la información como activo vital de las organizaciones sustenta el desarrollo del presente estudio, por cuanto aplicar una metodología mundialmente conocida como lo es MAGERIT permitirá a la empresa DECO INTERIORS SAC gestionar los riesgos a los que se enfrentan actualmente todos los activos, además de permitir la toma de decisiones de acuerdo a sus resultados.

Desde un punto de vista práctico, el producto del estudio impactará en el proceso de la organización, por cuanto una vez identificados los riesgos y amenazas, la empresa deberá poner en marcha los controles necesarios para minimizar el impacto de éstos en los activos. Al respecto, Carrasco (2005) mantiene que la justificación práctica de un trabajo investigativo valdrá para solucionar problemas prácticos.

Adicionalmente, como consecuencia de la falta de un método que consienta la seguridad de la información manifiesta por la empresa DECO INTERIORS SAC, aunado a la falta de modelamiento de los procesos, el estudio requerirá la elaboración del registro de activos y la evaluación del riesgo para determinar que decisiones tomar.

1.6. Hipótesis.

Si se aplica la Metodología Magerit V3, que tenga en cuenta la Cultura y Gestión de riesgo, así como la función del Recurso Humano, entonces se influirá de manera positiva en la seguridad de información de la empresa Deco Interiors SAC

1.7. Objetivos

1.7.1. Objetivos General

Determinar la influencia de la Metodología Magerit V3 en la seguridad de información de la empresa Deco Interiors SAC.

1.7.2. Objetivos Específicos

- a) Analizar epistemológicamente la influencia de la Metodología Magerit V3 en el proceso de Seguridad de la Información y su dinámica.
- b) Diagnosticar la influencia de la Metodología Magerit V3 en el estado actual de la seguridad de la información en la empresa Deco Interiors SAC.
- c) Determinar la influencia de la Metodología Magerit V3 en la mejora de la seguridad de la empresa Deco Interiors SAC.
- d) Evaluar la influencia de la Metodología Magerit V3 en los cambios provocados en la seguridad de información de la empresa Deco Interiors SAC.

1.8. Limitaciones

Representa una limitante el período de tiempo con el que se cuenta para desarrollar el proyecto que se plantea de gestión de riesgos esgrimiendo la metodología Magerit V3 en la en la empresa DECO INTERIORS SAC. A esto se suma, la limitación de recursos humanos por parte de la empresa con conocimientos sólidos acerca de la metodología. Otra limitación se atribuye a la falta de procesos documentados en todos los espacios funcionales de la empresa.

II. MATERIAL Y MÉTODO

2.1. Tipo y Diseño de Investigación.

Tipo de investigación: se desarrollará un trabajo investigativo de tipo aplicado, al respecto, Behar (2008) refiere que esta examina el uso de los conocimientos obtenidos. Expresa que la investigación aplicada se vincula de manera estrecha con la investigación básica, porque obedece a los resultados obtenidos y adelantos de la misma; por lo que la validación y justificación de la investigación aplicada requiere de un marco teórico; estableciéndose que pretende comparar la teoría con la realidad.

En el presente proyecto la investigación será de tipo aplicada por cuanto se pretende precisar de que manera influye la implementación de la metodología MAGERIT sobre la seguridad de la información de la empresa DECO INTERIORS SAC, para que a partir de los resultados la empresa tome la decisión de aplicarla y con ello asegurar sus activos de información.

Diseño de investigación: Aplicaremos un diseño correlacional descriptiva considerando que debemos determinar el vínculo o correlación que existe entre las variables en la misma unidad de investigación.

2.2. Población y muestra.

La población se encuentra detallada como un grupo definido o infinito de componentes o aspectos con las mismas particularidades sobre los que se pueden ampliar las conclusiones a las que llegue el investigador (Arias, 2012).

La empresa DECO INTERIORS SAC está dedicada a la comercialización de productos textiles como telas, lámparas, cortinas, papel tapiz, entre otros. Actualmente cuenta con un *staff* de 115 empleados, de las cuales 8 pertenecen al departamento de informática, por lo que serán los responsables del análisis que se realizará.

Respecto a la muestra, (Hernández et. al., 2014) la definen como una porción o subconjunto extraído de la población siendo esta representativa de la misma. En este caso particular la muestra se encontrará compuesta por las 8 personas que trabajan en el departamento de informática, los cuales pueden responder a los instrumentos de recaudación de datos por cuanto cuentan con el conocimiento para ello.

2.3. Variables, Operacionalización.

2.3.1. Variable independiente: Metodología MAGERIT

Las dimensiones de la variable Metodología MAGERIT son:

- Cultura de riesgo de información, cuyos indicadores son: Personal capacitado y Personal concientizado.
- Gestión de riesgos, cuyos indicadores son: Nivel de planeación, Nivel de Identificación y Nivel de Valoración.
- Infraestructura tecnológica, cuyos indicadores son: Disponibilidad tecnológica y Conectividad.
- Recursos humanos, cuyos indicadores son: nivel de pericia y nivel de conocimiento.

2.3.2. Variable dependiente: Seguridad de la información

La dimensión de la variable Seguridad de la información es:

- Seguridad, cuyos indicadores son: disponibilidad, autenticidad, integridad, trazabilidad y confidencialidad.

2.3.3. Operacionalización de las variables

Tabla 1.

Operacionalización de la Variable Independiente Metodología Magerit V3.

Variable	Definición	Dimensión	Indicadores	Ítems	Escala de medición y valores	Rangos % y niveles
Metodología Magerit	Metodología de análisis y gestión de riesgos de tecnologías de la información	Cultura de riesgo de información	• Personal capacitado	1, 2	<ul style="list-style-type: none"> • Nunca • Casi nunca • a veces • siempre • casi siempre 	1 – 49 = Bajo 50 – 77 = Moderado 78 – 100 = Alto
			• Personal concientizado	3, 4, 5		
			• Nivel de planeación	6, 7		
		Gestión de riesgos	• Nivel de identificación	8		
			• Nivel de valoración	9		
		Infraestructura tecnológica	• Disponibilidad tecnológica	10, 11, 12		
			• Conectividad	13		
		Recursos humanos	• Nivel de pericia	14		
			• Nivel de conocimiento	15, 16, 17, 18		

Nota. Elaboración propia.

Tabla 2.*Operacionalización de la variable dependiente seguridad de la información de la Empresa Deco Interiors*

Variable	Definición	Dimensión	Indicadores	Ítems	Escala de medición y valores	Rangos % y niveles
Seguridad de la información	Capacidad de las redes o sistemas de información para resistir, con un determinado nivel de confianza, los accidentes, acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad, trazabilidad y confidencialidad de los datos almacenados o transmitidos y de los servicios que dichas redes ofrecen o hacen accesibles.	Seguridad	• Confidencialidad	19	<ul style="list-style-type: none"> • Nunca • Casi nunca • a veces • siempre • casi siempre 	1 – 49 = Bajo 50 – 77 = Moderado 78 – 100 = Alto
			• Integridad	20		
			• Disponibilidad	21, 24, 25		
			• Autenticidad	22		
			• Trazabilidad	23		

Nota. Elaboración propia.

2.4. Técnicas e instrumentos de recaudación de datos, validez y confiabilidad.

Para la recaudación de datos del presente trabajo se requirió de lo siguiente:

- **Análisis Documental:** basado en esta técnica se podrá analizar el planteamiento de la metodología que se plantea sobre gestión de riesgos de la información de la organización en estudio.
- **Encuesta:** corresponde a una técnica de recaudación de datos, pues permite alcanzar una elevada recolección de información. Al respecto, Gallardo (2017) refiere que la encuesta forma esa técnica que lidera el estudio social por la versatilidad, provecho, imparcialidad y sencillez de las informaciones conseguidas.

Observación: Para complementar el llenado de las encuestas del Anexo N° 3.

- **Cuestionario;** Radica en una serie de preguntas de acuerdo a cada una de las variables que se medirán (Hernández et. al., 2014). Este instrumento, presentado en el anexo 3, será elaborado con base a las dimensiones e indicadores planteados y validado por expertos.
- **La validez;** corresponde a una propiedad que tiene el instrumento que le permite calcular de manera imparcial, específica, cierta y fidedigna lo que se pretende calcular de las variables examinadas (Gallardo, 2017). En el presente estudio, la veracidad del instrumento será obtenido por juicio de expertos el cual se muestra en el anexo 4.
- **La confiabilidad del instrumento;** esta propiedad depende de procedimientos de observación que detallan de manera minuciosa, lo que ocurre en determinado ambiente, valorando para ello el sitio, el momento y la situación estudiada, y así de esta manera poder conseguir el intercambio de opiniones con personas que investigan o evaluadores, en función a ello, la confiabilidad representará el grado de

correspondencia de las réplicas contempladas entre el entorno del individuo evaluado y de quien evalúa (Hernández et. al., 2014).

Tabla 3.

Confiabilidad

Coeficiente	Relación
0.00	Nula confiabilidad
0.70	Aceptable confiabilidad
0.90	Elevada confiabilidad
1.00	Máxima confiabilidad

Nota: Elaboración propia, Software utilizado SPSS 25

La confiabilidad será establecida mediante el coeficiente de Alfa de Cronbach, después de haberse registrado la información recolectada, en el sistema de estadística SPSS 25.

Confiabilidad variable 1: Metodología Magerit

Tabla 4.

Resumen de procesamiento de casos de la variable 1

		N	%
Casos	Válido	8	100,0
	Excluido*	0	,0
	Total	8	100,0

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

Nota: Elaboración propia, Software utilizado SPSS 25

Tabla 5.

Estadística de fiabilidad de la variable 1

Alfa de Cronbach	nº de elementos
0.912	18

Nota: Elaboración propia, Software utilizado SPSS 25

Acorde a los resultados mostrados por el sistema de estadística SPSS 25, es evidente que la confiabilidad de la variable Metodología Magerit es alta, cuyo valor es 0.912, como se indica en la tabla 5.

Confiabilidad variable 2: Seguridad de la información

Tabla 6.

Resumen de procesamiento de casos de la variable 2

		N	%
Casos	Válido	8	100,0
	Excluido*	0	,0
	Total	8	100,0

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

Nota: Elaboración propia, Software utilizado SPSS 25

Tabla 7.

Estadística de fiabilidad de la variable 2

Alfa de Cronbach	nº de elementos
0.909	7

Nota: Elaboración propia, Software utilizado SPSS 25

Acorde a los resultados mostrados por el sistema de estadística SPSS 25, es evidente que la confiabilidad de la variable Seguridad de la información es alta, cuyo valor es 0.909, como se indica en la tabla 7.

Confiabilidad variable 1 y 2

Tabla 8.

Resumen de procesamiento de casos de las variables 1 y 2

		N	%
Casos	Válido	8	100,0
	Excluido*	0	,0
	Total	8	100,0

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

Nota: Elaboración propia, Software utilizado SPSS 25

Tabla 9.

Estadística de fiabilidad de las variables 1 y 2

Alfa de Cronbach	nº de elementos
0.915	25

Nota: Elaboración propia, Software utilizado SPSS 25

Los resultados arrojados por el sistema de estadística SPSS 25 evidencian que la confiabilidad de las variables Metodología Magerit y Seguridad de la información es alta, con un valor de confiabilidad de 0,915, como se muestra en la tabla 9.

2.5. Procedimientos de análisis de datos.

En el proceso del resultado obtenido donde se aplicará el instrumento, será empleada la técnica de la estadística inferencial, descriptiva y la prueba de correlación de Pearson, mediante el sistema SPSS 25.

2.6. Criterios éticos

Según el Informe Belmont, los principios éticos fundamentales en una investigación son:

- **Respecto;** el cual se brindará a las personas que den contestación al instrumento elaborado. Esto implica que sus respuestas no serán modificadas ni alteradas y que los resultados serán reconocidos como base del estudio realizado. Y, finalmente, no se estimulará actitudes que condicionen las contestaciones de las personas que participaron.
- **Beneficencia;** con este principio se busca incrementar al máximo los potenciales beneficios para la organización y su personal a la vez que se disminuyen los riesgos de la seguridad de la información.
- **Justicia;** en el estudio planteado no se expone a riesgos a ninguno de los participantes.

2.7. Criterios de Rigor científico.

En el desarrollo de esta investigación cuantitativa se aplicarán los subsiguientes principios de rigor científico:

- **Objetividad:** Grado en el cual el estudio se encuentra exento de la influencia de la visión de quien investiga (Guba, 1981). Para indicar que el estudio se realiza sin influencia por parte de quien lo desarrolla, ya que el principal propósito es la finalización de un proyecto de grado.
- **Validez externa:** Grado en el cual logran aplicarse los hallazgos de una investigación a diferentes individuos o situaciones (Guba, 1981). A partir de esta definición se agrega de acuerdo a los resultados conseguidos los ejecutivos de la empresa tomarán o no la decisión de implementar la metodología para disminuir el riesgo de sus activos de información.
- **Fiabilidad:** Estado en el cual los instrumentos repiten iguales medidas en y en iguales escenarios (Guba, 1981). Este principio es demostrado con los resultados derivados de la confiabilidad del instrumento.

III. RESULTADOS

Para la investigación una vez analizada la fundamentación teórica de la metodología Magerit, se aplicaron los conceptos de cómo gestionar los riesgos, en cuanto a definir que posee la organización y que pasaría si continúa en el mismo estado. Por ello se utilizó una encuesta formulando interrogantes relacionadas al contexto. A continuación, se analiza el resultado obtenido en cada una de las preguntas:

3.1. Análisis descriptivo

Tabla 10.

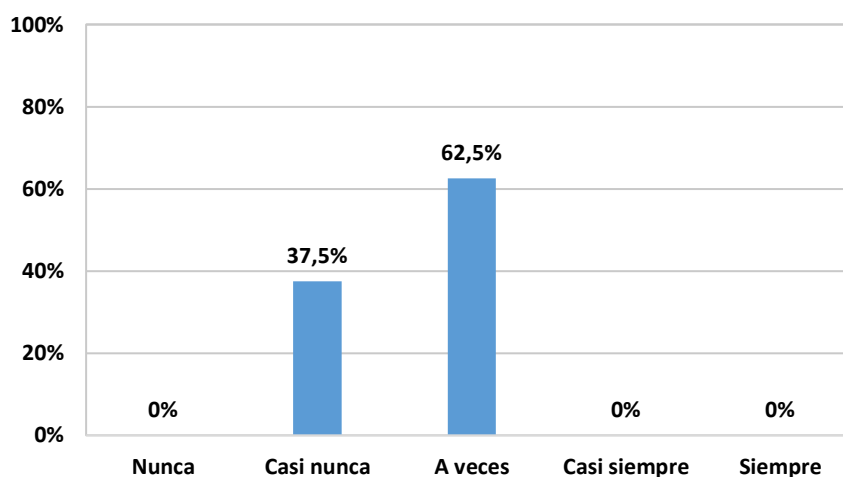
¿La empresa le ha proporcionado capacitación sobre el resguardo de la información que administra?

	Opciones de respuesta	Frecuencia	%	% Válido	% acumulado
Válido	Nunca	0	0	0	0
	Casi nunca	3	37.5	37.5	37.5
	A veces	5	62.5	62.5	100
	Casi siempre	0	0	0	
	Siempre	0	0	0	
	Total	8	100	100	

Nota: Elaboración propia

Figura 3.

Ítem 1. ¿La empresa le ha proporcionado capacitación sobre el resguardo de la información que administra?



Nota: Elaboración propia

Se muestran los resultados en la tabla 10 y figura 3 que el 62.5% del personal del área de informática sólo a veces ha recibido capacitación por parte de la empresa respecto al resguardo de la información que administra, el restante 37.5% expresa que casi nunca esa acción ha sido realizada.

Tabla 11.

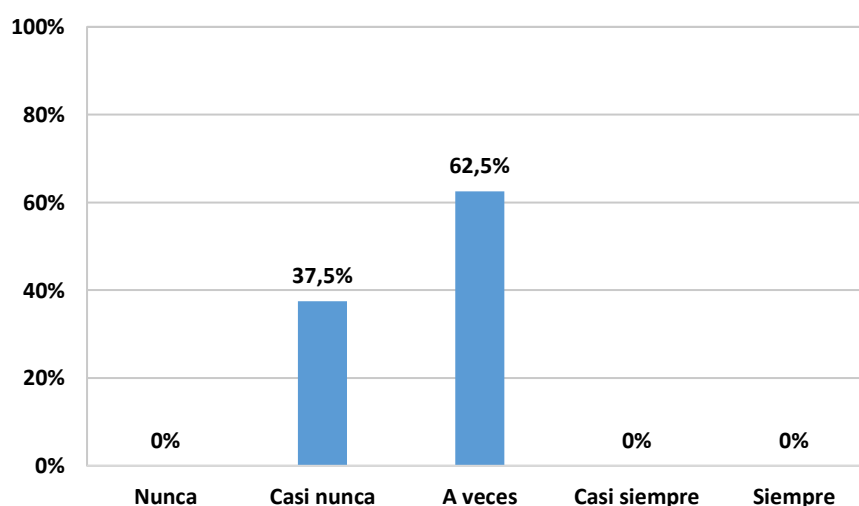
Ítem 2. ¿La empresa le ha proporcionado información sobre los riesgos tecnológicos de la información que administra?

	Opciones de respuesta	Frecuencia	%	% Válido	% acumulado
Válido	Nunca	0	0	0	0
	Casi nunca	3	37.5	37.5	37.5
	A veces	5	62.5	62.5	100
	Casi siempre	0	0	0	
	Siempre	0	0	0	
	Total		8	100	100

Nota: Elaboración propia

Figura 4.

Ítem 2. ¿La empresa le ha proporcionado información sobre los riesgos tecnológicos de la información que administra?



Nota: Elaboración propia

Los resultados de la tabla 11 y figura 4 muestra que el 62.5% de empleados del área de informática sólo a veces he recibido información por parte de la empresa respecto a los riesgos tecnológicos de la información que administra, el restante 37.5% expresa que casi nunca esa acción ha sido realizada.

Tabla 12.

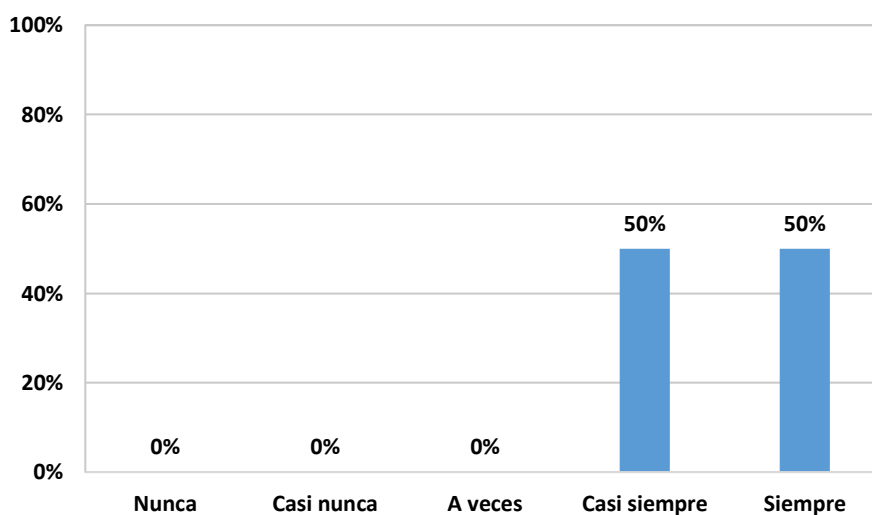
Ítem 3. ¿Pone en práctica alguna estrategia para la protección de la información?

	Opciones de respuesta	Frecuencia	%	% Válido	% acumulado
Válido	Nunca	0	0	0	0
	Casi nunca	0	0	0	0
	A veces	0	0	0	0
	Casi siempre	4	50	50	50
	Siempre	4	50	50	100
	Total	8	100	100	

Nota: Elaboración propia

Figura 5.

Ítem 3. ¿Pone en práctica alguna estrategia para la protección de la información?



Nota: Elaboración propia

Los resultados de la tabla 12 y figura 5 muestra que el 50% de empleados del área de informática siempre pone en práctica alguna estrategia para la protección de la información, el restante 50% expresa que casi siempre lo hace.

Tabla 13.

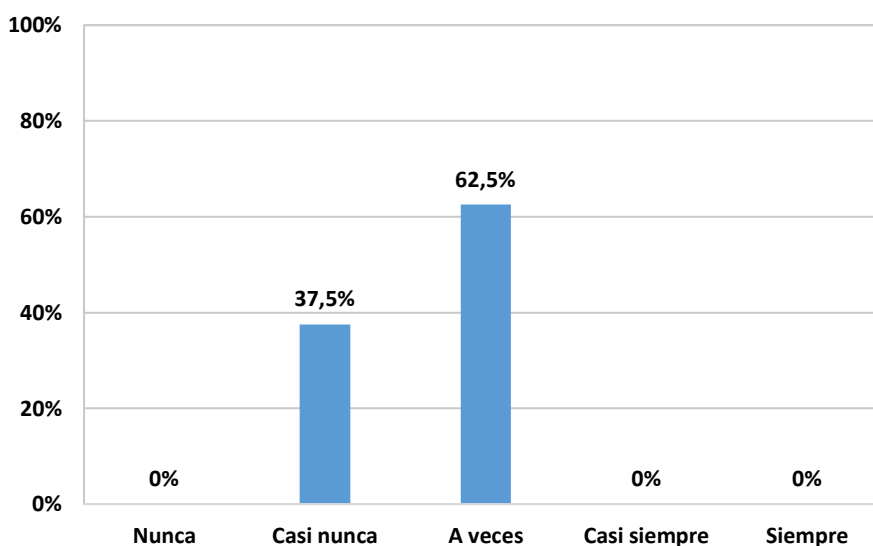
Ítem 4. ¿La empresa ha implementado alguna estrategia para concientizar al personal sobre los riesgos e importancia de los activos de información?

	Opciones de respuesta	Frecuencia	%	% Válido	% acumulado
Válido	Nunca	0	0	0	0
	Casi nunca	3	37.5	37.5	37.5
	A veces	5	62.5	62.5	100
	Casi siempre	0	0	0	
	Siempre	0	0	0	
	Total		8	100	100

Nota: Elaboración propia

Figura 6.

Ítem 4. ¿La empresa ha implementado alguna estrategia para concientizar al personal sobre los riesgos e importancia de los activos de información?



Nota: Elaboración propia

Los resultados de la tabla 13 y figura 6 muestra que el 62.5% de empleados del área de informática señala que sólo a veces la empresa ha implementado estrategias para concientizar al personal sobre los riesgos e importancia de los activos de información, el restante 37.5% expresa que casi nunca han realizado tal acción.

Tabla 14.

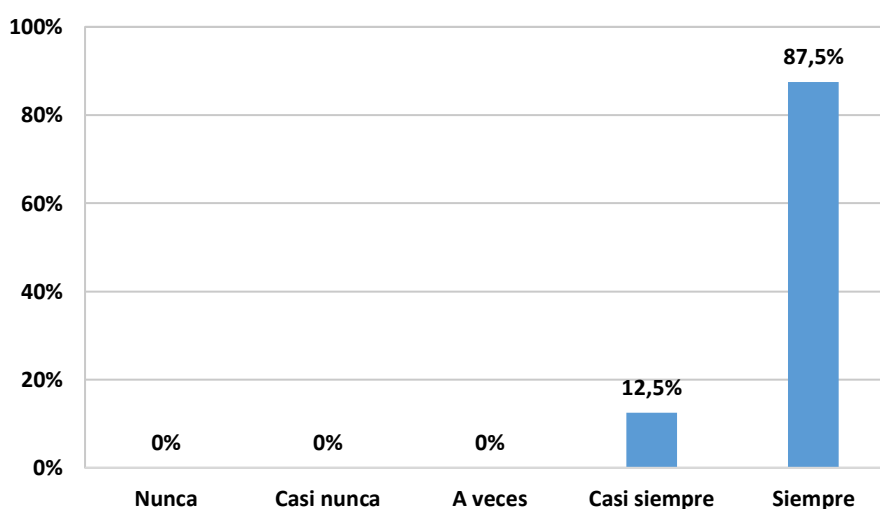
Ítem 5. ¿Se considera comprometido con el resguardo de la información que administra?

	Opciones de respuesta	Frecuencia	%	% Válido	% acumulado
Válido	Nunca	0	0	0	0
	Casi nunca	0	0	0	0
	A veces	0	0	0	0
	Casi siempre	1	12.5	12.5	12.5
	Siempre	7	87.5	87.5	100
	Total		8	100	100

Nota: Elaboración propia

Figura 7.

Ítem 5. ¿Se considera comprometido con el resguardo de la información que administra?



Nota: Elaboración propia

Los resultados de la tabla 14 y figura 7 muestra que el 87.5% de empleados del área de informática señala estar siempre comprometido con el resguardo de la información que administra, mientras que el 12.5% señala que casi siempre lo está.

Tabla 15.

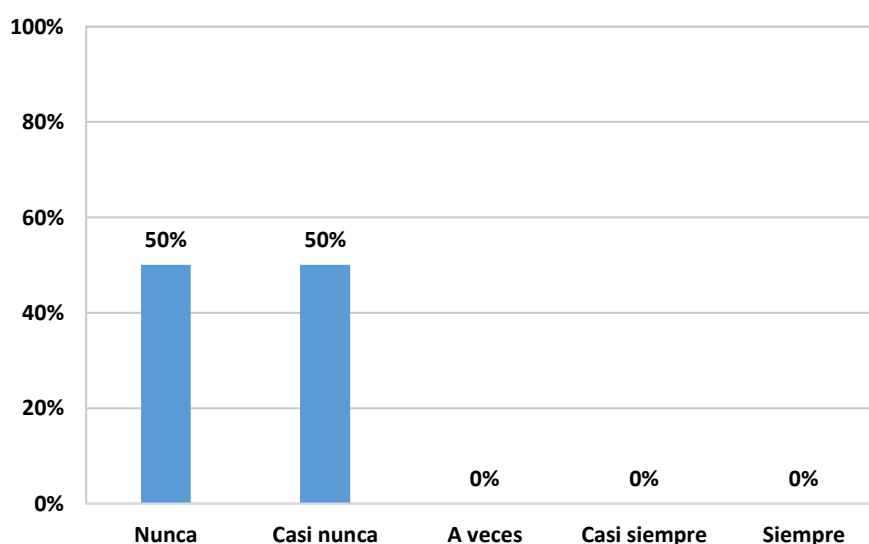
Ítem 6. ¿La empresa ha implementado alguna estrategia para evaluar los riesgos a los que está sometida la información?

	Opciones de respuesta	Frecuencia	%	% Válido	% acumulado
Válido	Nunca	4	50	50	50
	Casi nunca	4	50	50	100
	A veces	0	0	0	
	Casi siempre	0	0	0	
	Siempre	0	0	0	
	Total		8	100	100

Nota: Elaboración propia

Figura 8.

Ítem 6. ¿La empresa ha implementado alguna estrategia para evaluar los riesgos a los que está sometida la información?



Nota: Elaboración propia

La tabla 15 y figura 8 indican que el 50% de empleados del área de informática señala que la empresa nunca ha implementado alguna estrategia para evaluar el riesgo al que está sometida la información, el restante 50% expresa que sólo casi nunca han llevado a cabo tal acción.

Tabla 16.

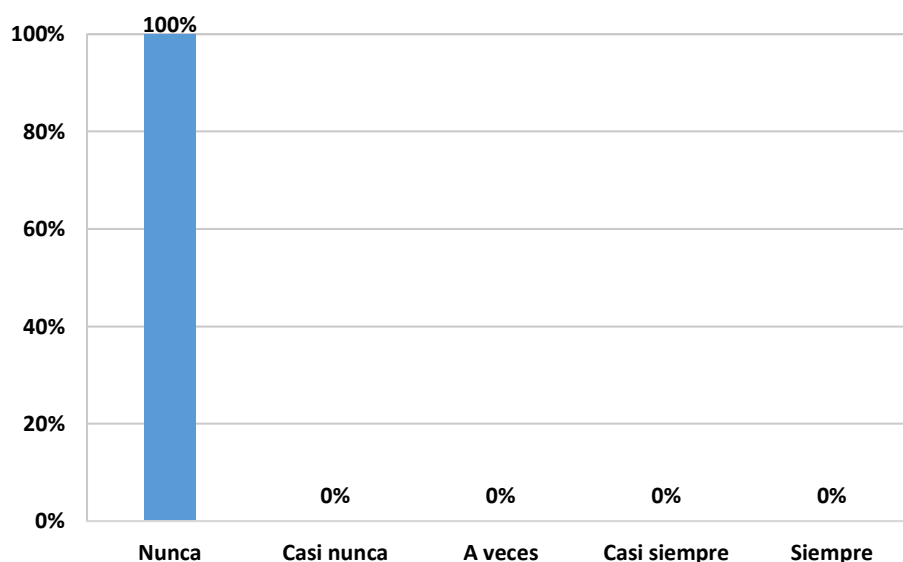
Ítem 7. ¿La empresa ha determinado los riesgos a los que están sometidos los activos de información?

	Opciones de respuesta	Frecuencia	%	% Válido	% acumulado
Válido	Nunca	8	100	100	100
	Casi nunca	0	0	0	
	A veces	0	0	0	
	Casi siempre	0	0	0	
	Siempre	0	0	0	
	Total		8	100	100

Nota: Elaboración propia

Figura 9.

Ítem 7. ¿La empresa ha determinado los riesgos a los que están sometidos los activos de información?



Nota: Elaboración propia

Los resultados de la tabla 16 y figura 9 indica el 100% de los empleados del área de informática señala que la empresa no ha determinado el riesgo al que están sometidos los activos de información.

Tabla 17.

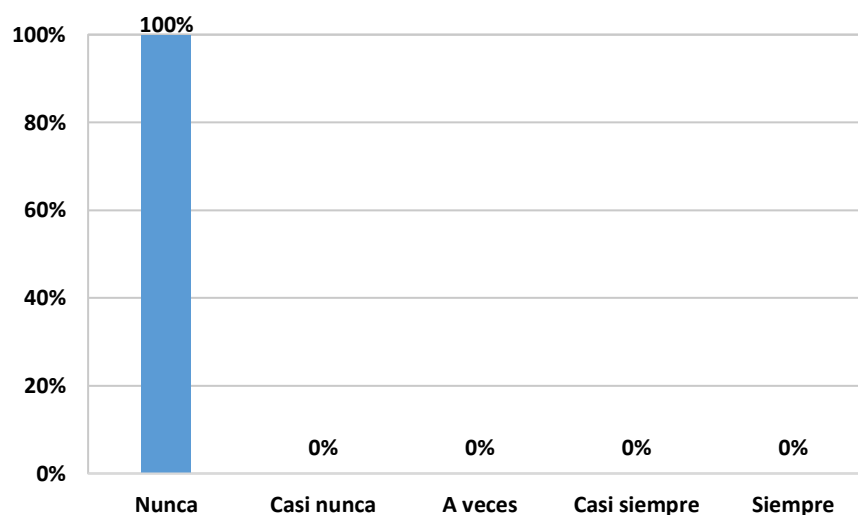
Ítem 8. ¿La empresa ha identificado los riesgos sobre la información que afectarían las labores diarias?

	Opciones de respuesta	Frecuencia	%	% Válido	% acumulado
Válido	Nunca	8	100	100	100
	Casi nunca	0	0	0	
	A veces	0	0	0	
	Casi siempre	0	0	0	
	Siempre	0	0	0	
	Total		8	100	100

Nota: Elaboración propia

Figura 10.

Ítem 8. ¿La empresa ha identificado los riesgos sobre la información que afectarían las labores diarias?



Nota: Elaboración propia

La tabla 17 y figura 10 muestran que el 100% de los empleados del área de informática señala que en la empresa no se han identificado los riesgos sobre la información que afectarían las labores diarias.

Tabla 18.

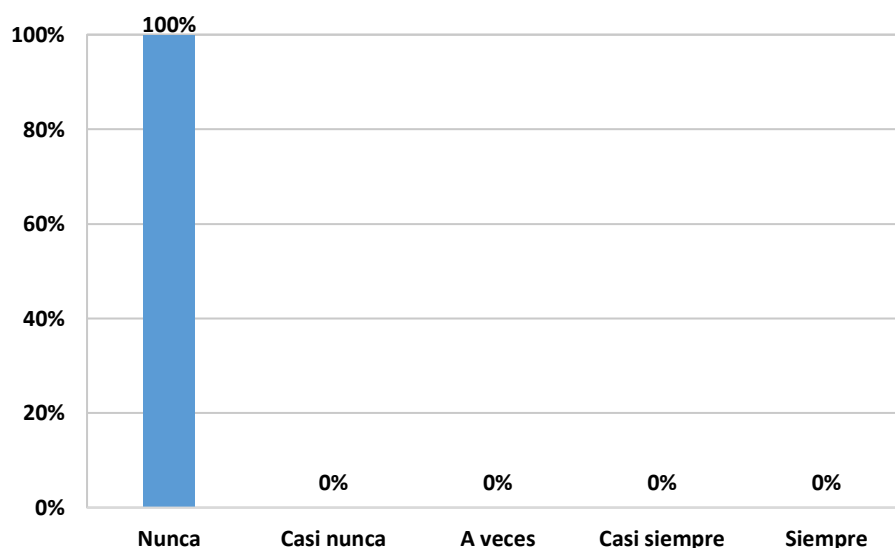
Ítem 9. ¿Se han cuantificado en la empresa los posibles daños en los activos de información?

	Opciones de respuesta	Frecuencia	%	% Válido	% acumulado
Válido	Nunca	8	100	100	100
	Casi nunca	0	0	0	
	A veces	0	0	0	
	Casi siempre	0	0	0	
	Siempre	0	0	0	
	Total		8	100	100

Nota: Elaboración propia

Figura 11.

Ítem 9. ¿Se han cuantificado en la empresa los posibles daños en los activos de información?



Nota: Elaboración propia

La tabla 18 y figura 11 indican que el 100% de empleados del área de informática señala que en la empresa no se han cuantificado los posibles daños en los activos de información.

Tabla 19.

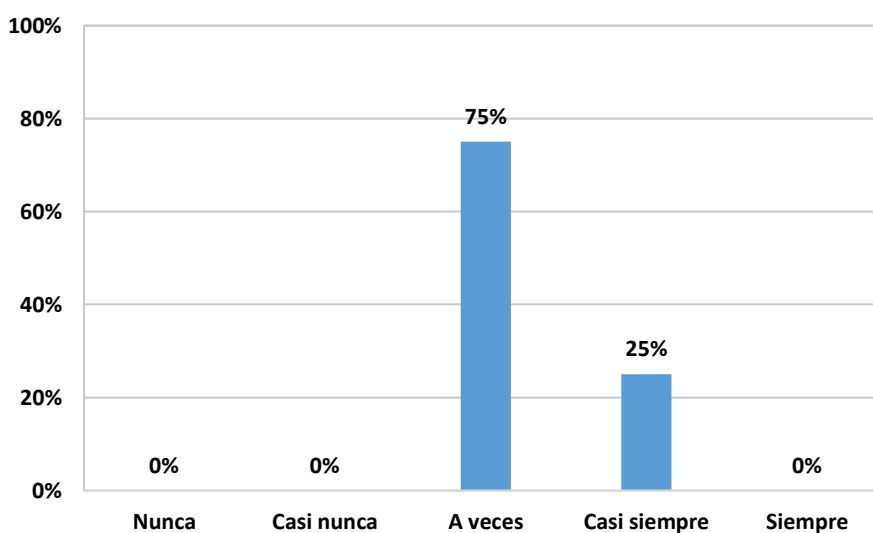
Ítem 10. ¿La tecnología de información disponible en la empresa es adecuada para el desarrollo de las actividades?

	Opciones de respuesta	Frecuencia	%	% Válido	% acumulado
Válido	Nunca	0	0	0	0
	Casi nunca	0	0	0	0
	A veces	6	75	75	75
	Casi siempre	2	25	25	100
	Siempre	0	0	0	
	Total	8	100	100	

Nota: Elaboración propia

Figura 12.

Ítem 10. ¿La tecnología de información disponible en la empresa es adecuada para el desarrollo de las actividades?



Nota: Elaboración propia

La tabla 19 y figura 12 presentan que el 75% de los empleados del área de informática señala que sólo a veces la tecnología de información disponible en la empresa es apropiada para el avance de las operaciones, entretanto que el 25% restante indica que casi siempre es adecuada.

Tabla 20.

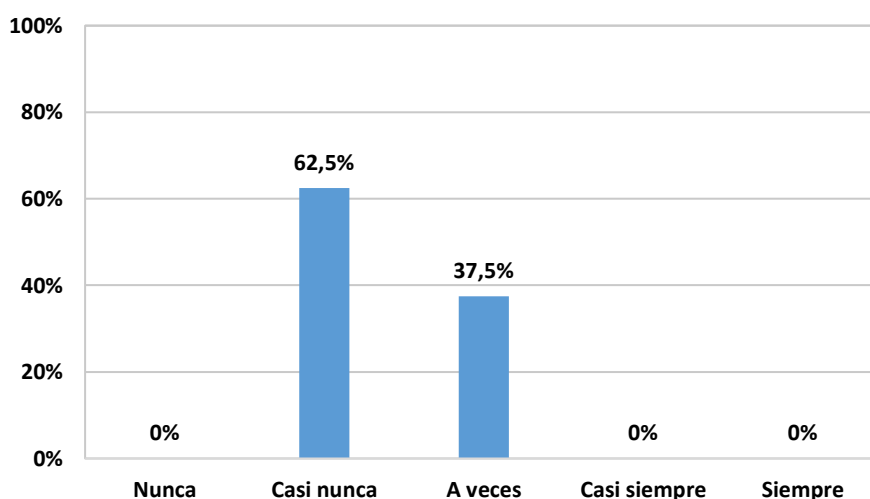
Ítem 11. ¿La tecnología de información disponible en la empresa garantiza la seguridad de la información?

	Opciones de respuesta	Frecuencia	%	% Válido	% acumulado
Válido	Nunca	0	0	0	0
	Casi nunca	5	62.5	62.5	62.5
	A veces	3	37.5	37.5	100
	Casi siempre	0	0	0	
	Siempre	0	0	0	
	Total		8	100	100

Nota: Elaboración propia

Figura 13.

Ítem 11. ¿La tecnología de información disponible en la Empresa garantiza la seguridad de la información?



Nota: Elaboración propia

La tabla 20 y figura 13 muestran que el 62.5% de los empleados del área de informática señala que casi nunca la tecnología de información disponible en la empresa garantiza la seguridad de la información, entretanto el 37.5% demás indica que sólo a veces lo es.

Tabla 21.

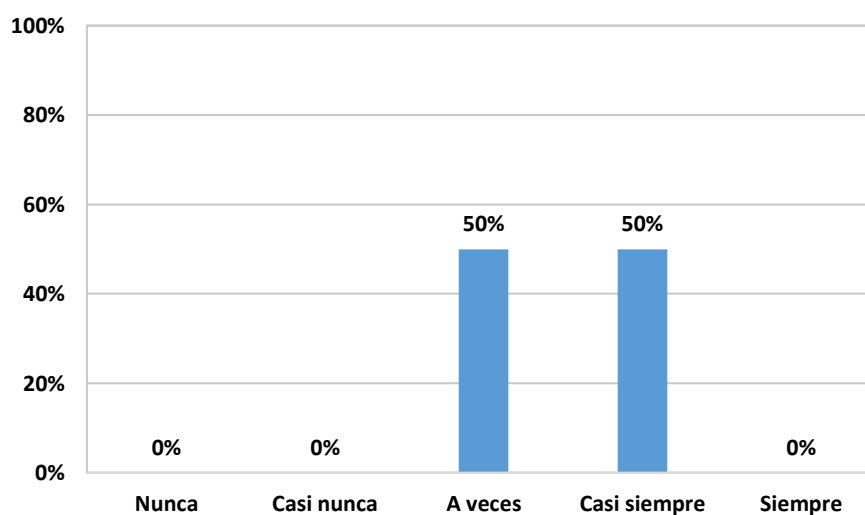
Ítem 12. ¿El servicio de internet disponible en la empresa es adecuado para llevar a cabo sus actividades?

	Opciones de respuesta	Frecuencia	%	% Válido	% acumulado
Válido	Nunca	0	0	0	0
	Casi nunca	0	0	0	0
	A veces	4	50	50	50
	Casi siempre	4	50	50	100
	Siempre	0	0	0	
	Total	8	100	100	

Nota: Elaboración propia

Figura 14.

Ítem 12. ¿El servicio de internet disponible en la empresa es adecuado para llevar a cabo sus actividades?



Nota: Elaboración propia

Los resultados de la tabla 21 y figura 14 muestra que el 50% de empleados del área de informática señala que sólo a veces el servicio de internet disponible en la empresa es adecuado para llevar a cabo sus actividades, mientras que el 50% restante indica que casi siempre lo es.

Tabla 22.

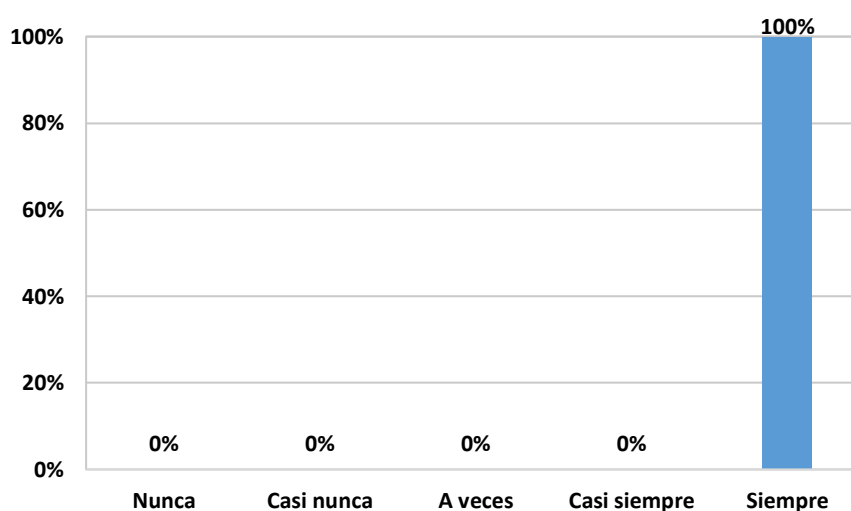
Ítem 13. ¿Las computadoras están conectadas con la red para enviar y recibir información?

	Opciones de respuesta	Frecuencia	%	% Válido	% acumulado
Válido	Nunca	0	0	0	0
	Casi nunca	0	0	0	0
	A veces	0	0	0	0
	Casi siempre	0	0	0	0
	Siempre	8	100	100	100
	Total	8	100	100	

Nota: Elaboración propia

Figura 15.

Ítem 13. ¿Las computadoras están conectadas con la red para enviar y recibir información?



Nota: Elaboración propia

Los resultados de la tabla 22 y figura 15 muestra que el 100% de empleados del área de informática señala que siempre las computadoras están conectadas con la red para enviar y recibir información.

Tabla 23.

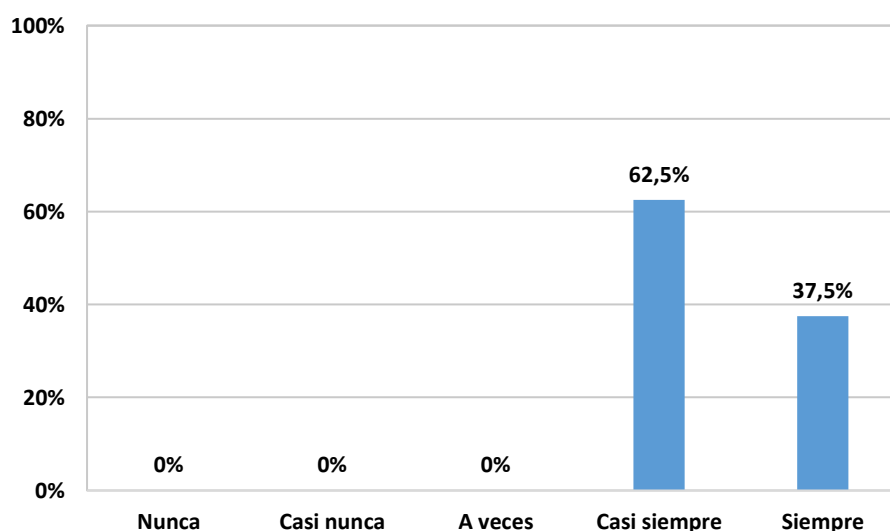
Ítem 14. ¿Su nivel de pericia le permite realizar un adecuado aseguramiento de la información que administra?

	Opciones de respuesta	Frecuencia	%	% Válido	% acumulado
Válido	Nunca	0	0	0	0
	Casi nunca	0	0	0	0
	A veces	0	0	0	0
	Casi siempre	5	62.5	62.5	50
	Siempre	3	37.5	37.5	100
	Total	8	100	100	

Nota: Elaboración propia

Figura 16.

Ítem 14. ¿Su nivel de pericia le permite realizar un adecuado aseguramiento de la información que administra?



Nota: Elaboración propia

Los resultados de la tabla 23 y figura 16 muestra que el 62.5% de empleados del área de informática señala que casi siempre su nivel de pericia le permite realizar un adecuado aseguramiento de la información que administra, mientras que el 37.5% restante indica que siempre se lo permite.

Tabla 24.

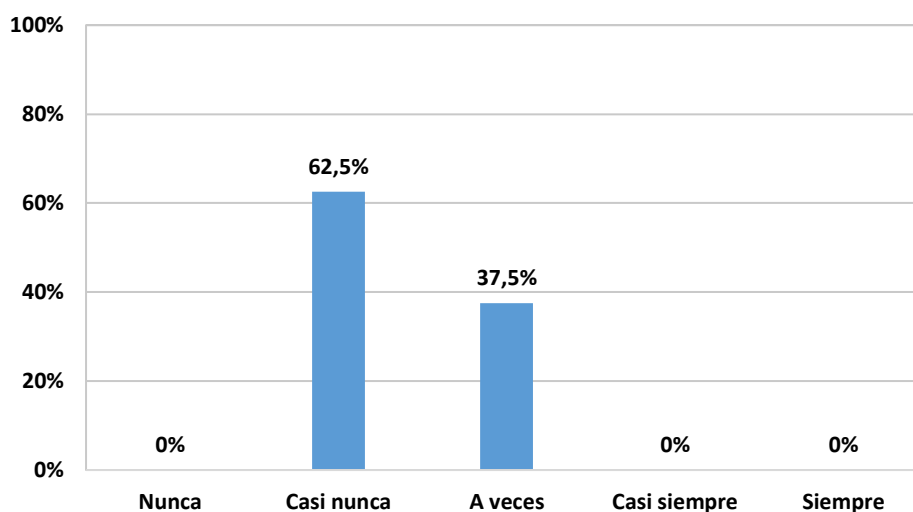
Ítem 15. ¿Requiere de algún tipo de asistencia para resolver problemas informáticos durante sus labores diarias?

	Opciones de respuesta	Frecuencia	%	% Válido	% acumulado
Válido	Nunca	0	0	0	0
	Casi nunca	5	62.5	62.5	62.5
	A veces	3	37.5	37.5	100
	Casi siempre	0	0	0	
	Siempre	0	0	0	
	Total		8	100	100

Nota: Elaboración propia

Figura 17. *Ítem 15. ¿Requiere de algún tipo de asistencia para resolver problemas i*

formáticos durante sus labores diarias?



Nota: Elaboración propia

Los resultados de la tabla 24 y figura 17 muestra que el 62.5% de empleados del área de informática señala que casi nunca requiere de algún tipo de asistencia para resolver problemas informáticos durante sus labores diarias, mientras que el 37.5% restante indica que a veces lo requiere.

Tabla 25.

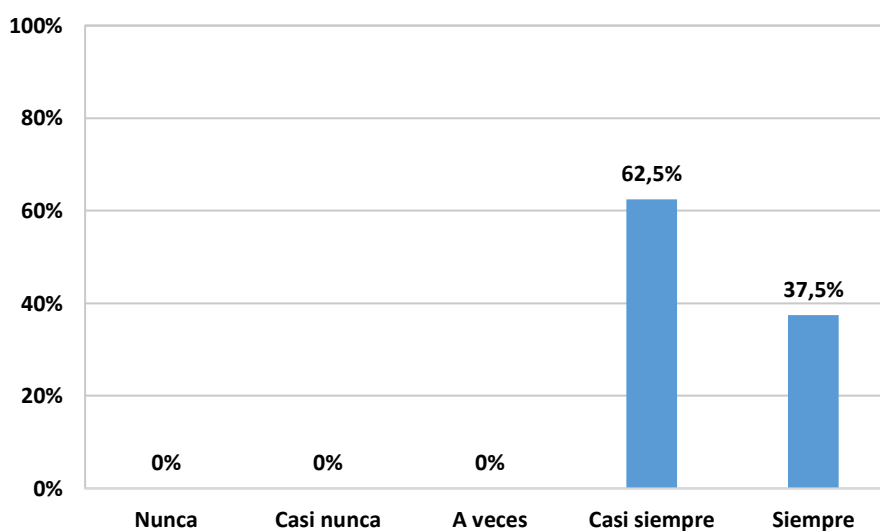
Ítem 16. ¿El servicio de internet le permite ingresar a todas las páginas web que desee?

	Opciones de respuesta	Frecuencia	%	% Válido	% acumulado
Válido	Nunca	0	0	0	0
	Casi nunca	5	62.5	62.5	62.5
	A veces	3	37.5	37.5	100
	Casi siempre	0	0	0	
	Siempre	0	0	0	
	Total		8	100	100

Nota: Elaboración propia

Figura 18.

Ítem 16. ¿El servicio de internet le permite ingresar a todas las páginas web que desee?



Nota: Elaboración propia

La tabla 25 y figura 18 muestran que el 62.5% de los empleados del área de informática señala que casi siempre el servicio de internet le permite ingresar a todas las páginas web que desee, mientras que el 37.5% restante indica que siempre se lo permite.

Tabla 26.

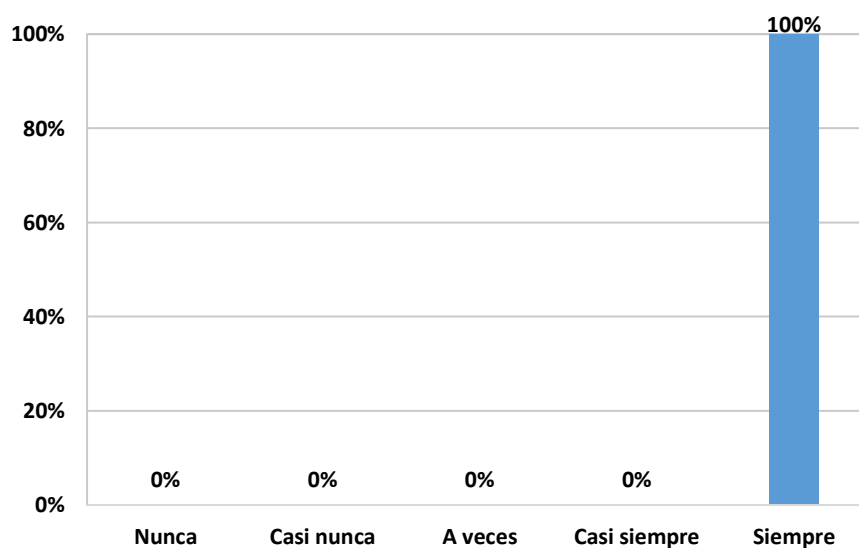
Ítem 17. ¿Puede recibir y enviar correos desde su computadora de trabajo?

	Opciones de respuesta	Frecuencia	%	% Válido	% acumulado
Válido	Nunca	0	0	0	0
	Casi nunca	0	0	0	0
	A veces	0	0	0	0
	Casi siempre	0	0	0	0
	Siempre	8	100	100	100
	Total	8	100	100	

Nota: Elaboración propia

Figura 19.

Ítem 17. ¿Puede recibir y enviar correos desde su computadora de trabajo?



Nota: Elaboración propia

Los resultados de la tabla 26 y figura 19 muestra que el 100% de empleados del área de informática señala que siempre puede recibir y enviar correos desde su computadora de trabajo.

Tabla 27.

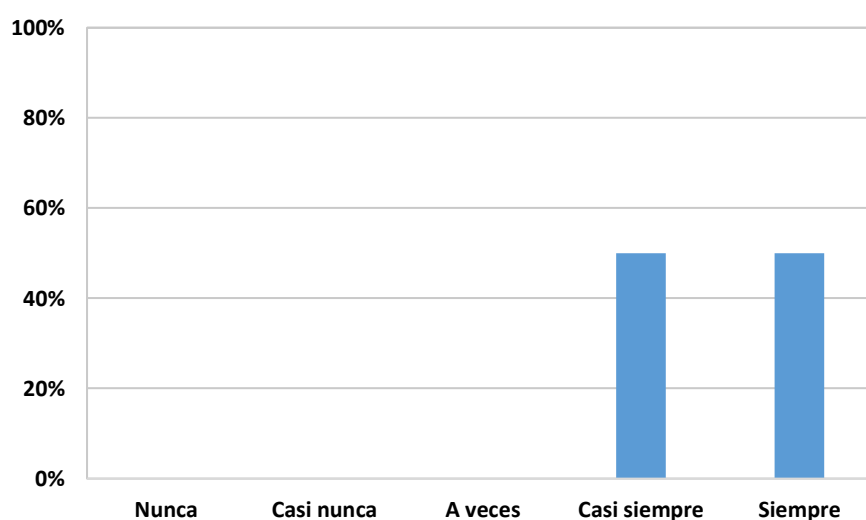
Ítem 18. ¿Considera que su nivel de conocimiento en el manejo de la tecnología informática, es sólido?

	Opciones de respuesta	Frecuencia	%	% Válido	% acumulado
Válido	Nunca	0	0	0	0
	Casi nunca	0	0	0	0
	A veces	0	0	0	0
	Casi siempre	4	50	50	50
	Siempre	4	50	50	100
	Total	8	100	100	

Nota: Elaboración propia

Figura 20.

Ítem 18. ¿Considera que su nivel de conocimiento en el manejo de la tecnología informática es sólido?



Nota: Elaboración propia

En la tabla 27 y figura 20 se muestra que el 50% de los empleados del área de informática señala que casi siempre su nivel de conocimiento en el manejo de la tecnología informática es sólido, el restante 50% refiere que siempre su nivel de conocimiento al respecto es sólido.

Tabla 28.

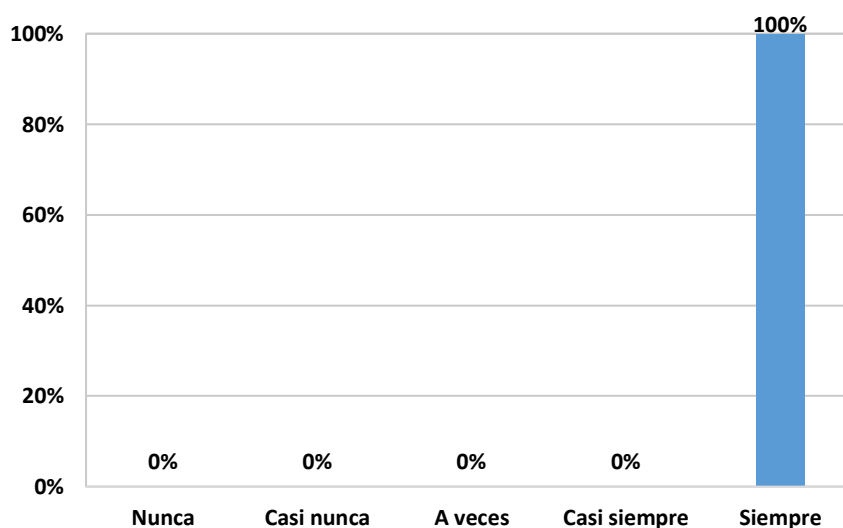
Ítem 19. ¿La empresa ha establecido políticas o procedimientos para asegurar la confidencialidad de la información?

	Opciones de respuesta	Frecuencia	%	% Válido	% acumulado
Válido	Nunca	0	0	0	0
	Casi nunca	0	0	0	0
	A veces	0	0	0	0
	Casi siempre	0	0	0	0
	Siempre	8	100	100	100
	Total	8	100	100	

Nota: Elaboración propia

Figura 21.

Ítem 19. ¿La empresa ha establecido políticas o procedimientos para asegurar la confidencialidad de la información?



Nota: Elaboración propia

Los resultados de la tabla 28 y figura 21 muestra que el 100% de empleados del área de informática señala que la organización siempre ha establecido políticas o procedimientos que aseguren la confidencialidad de la información.

Tabla 29.

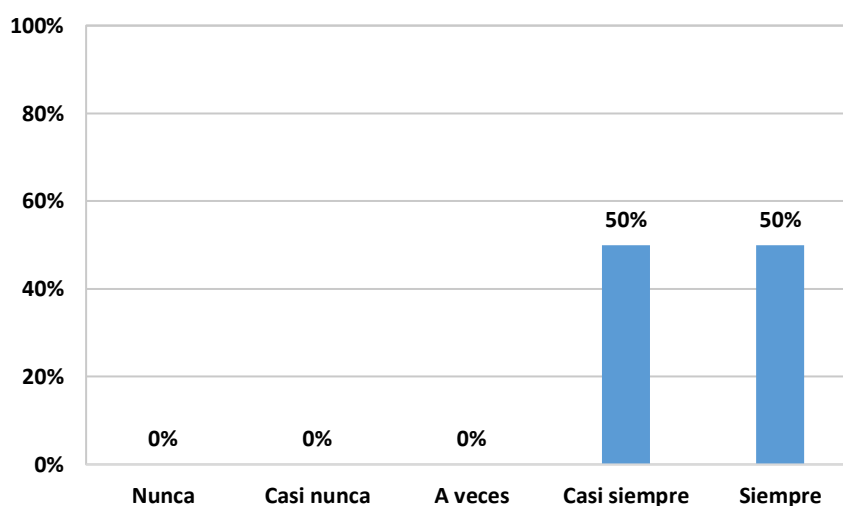
Ítem 20. ¿La empresa ha establecido políticas o procedimientos para asegurar la integridad de la información?

	Opciones de respuesta	Frecuencia	%	% Válido	% acumulado
Válido	Nunca	0	0	0	0
	Casi nunca	0	0	0	0
	A veces	0	0	0	0
	Casi siempre	4	50	50	50
	Siempre	4	50	50	100
	Total	8	100	100	

Nota: Elaboración propia

Figura 22.

Ítem 20. ¿La empresa ha establecido políticas o procedimientos para asegurar la integridad de la información?



Nota: Elaboración propia

Los resultados de la tabla 29 y figura 22 muestra que el 50% de empleados del área de informática señala que la empresa casi siempre ha establecido políticas o diferentes formas que aseguren la integridad de la información, el 50% restante expresa que dichas políticas se establecen siempre.

Tabla 30.

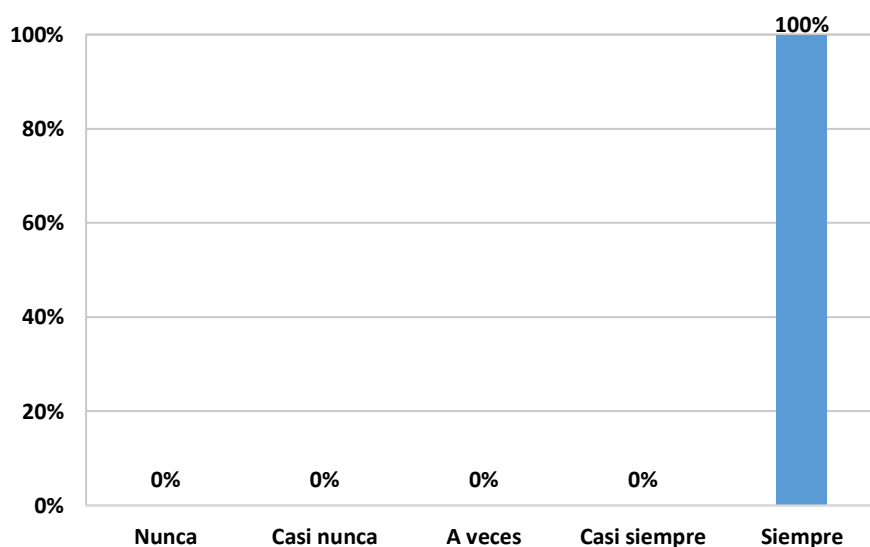
Ítem 21. ¿La empresa ha establecido políticas o procedimientos para asegurar la disponibilidad de la información?

	Opciones de respuesta	Frecuencia	%	% Válido	% acumulado
Válido	Nunca	0	0	0	0
	Casi nunca	0	0	0	0
	A veces	0	0	0	0
	Casi siempre	0	0	0	0
	Siempre	8	100	100	100
	Total	8	100	100	

Nota: Elaboración propia

Figura 23.

Ítem 21. ¿La empresa ha establecido políticas o procedimientos para asegurar la disponibilidad de la información?



Nota: Elaboración propia

Los resultados de la tabla 30 y figura 23 muestra que el 100% de empleados del área de informática señala que la empresa siempre ha establecido políticas o procesos que aseguren la disponibilidad de la información.

Tabla 31.

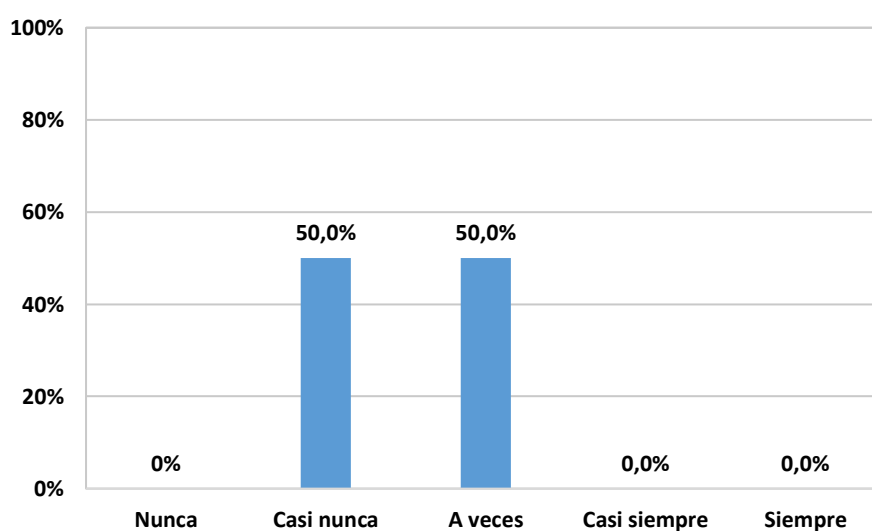
Ítem 22. ¿La empresa ha establecido políticas o procedimientos para verificar la autenticidad de la información?

	Opciones de respuesta	Frecuencia	%	% Válido	% acumulado
Válido	Nunca	0	0	0	0
	Casi nunca	4	50	50	50
	A veces	4	50	50	100
	Casi siempre	0	0	0	0
	Siempre	0	0	0	0
	Total	8	100	100	

Nota: Elaboración propia

Figura 24.

Ítem 22. ¿La empresa ha establecido políticas o procedimientos para verificar la autenticidad de la información?



Nota: Elaboración propia

Los resultados de la tabla 31 y figura 24 muestra que el 50% de empleados del área de informática señala que la empresa casi nunca ha establecido políticas o procedimientos para verificar la autenticidad de la información, por su parte, el 50% restante indica que sólo a veces se verifica la autenticidad.

Tabla 32.

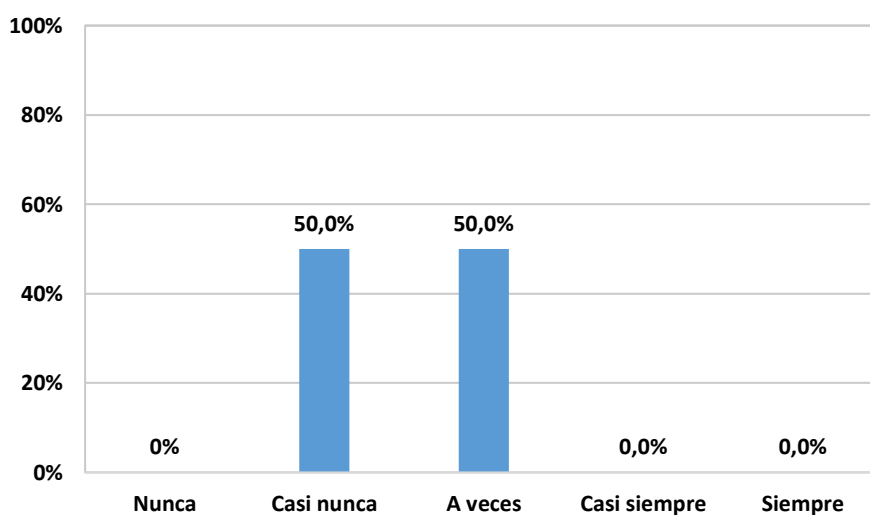
Ítem 23. ¿La empresa ha establecido políticas o procedimientos para verificar la trazabilidad de la información?

	Opciones de respuesta	Frecuencia	%	% Válido	% acumulado
Válido	Nunca	0	0	0	0
	Casi nunca	4	50	50	50
	A veces	4	50	50	100
	Casi siempre	0	0	0	0
	Siempre	0	0	0	0
	Total		8	100	100

Nota: Elaboración propia

Figura 25.

Ítem 23. ¿La empresa ha establecido políticas o procedimientos para verificar la trazabilidad de la información?



Nota: Elaboración propia

Los resultados de la tabla 32 y figura 25 muestra que el 50% de empleados del área de informática señala que la organización casi nunca ha establecido políticas o procedimientos para verificar la trazabilidad de la información, por su parte, el 50% restante indica que sólo a veces se verifica la trazabilidad.

Tabla 33.

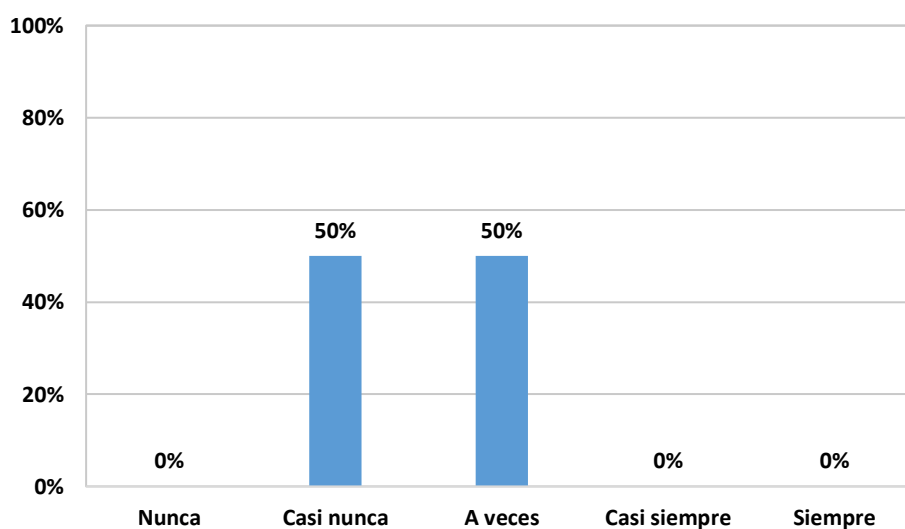
Ítem 24. ¿Existe algún procedimiento para resolver situaciones inesperadas de pérdida de información?

	Opciones de respuesta	Frecuencia	%	% Válido	% acumulado
Válido	Nunca	0	0	0	0
	Casi nunca	4	50	50	50
	A veces	4	50	50	100
	Casi siempre	0	0	0	0
	Siempre	0	0	0	0
	Total	8	100	100	

Nota: Elaboración propia

Figura 26.

Ítem 24. ¿Existe algún procedimiento para resolver situaciones inesperadas de pérdida de información?



Nota: Elaboración propia

Los resultados de la tabla 33 y figura 26 muestra que el 50% de empleados del área de informática señala que la empresa casi nunca existe un procedimiento para resolver situaciones inesperadas de pérdida de información, por su parte, el 50% restante indica que sólo a veces se puede disponer de ese procedimiento.

Tabla 34.

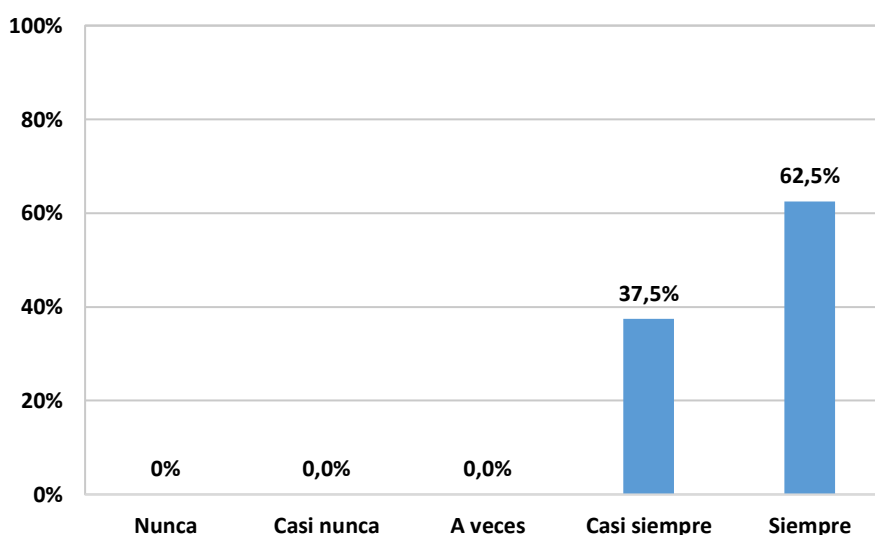
Ítem 25. ¿Se llevan a cabo respaldos de la información de la empresa como estrategia de resguardo y aseguramiento de la información?

	Opciones de respuesta	Frecuencia	%	% Válido	% acumulado
Válido	Nunca	0	0	0	0
	Casi nunca	0	0	0	0
	A veces	0	0	0	0
	Casi siempre	3	37.5	37.5	37.5
	Siempre	5	62.5	62.5	100
	Total	8	100	100	

Nota: Elaboración propia

Figura 27.

Ítem 25. ¿Se llevan a cabo respaldos de la información de la empresa como estrategia de resguardo y aseguramiento de la información?



Nota: Elaboración propia

La tabla 34 y figura 27 muestran que el 62.5% de los empleados del área de informática señala que en la empresa siempre se llevan a cabo respaldos de la información como estrategia de resguardo y aseguramiento de la información, por su parte, el 32.5% restante indica que sólo a veces se realizan dichas acciones.

Al analizar el resultado global obtenido sólo el 62.5% de las personas a veces han sido capacitados, la empresa le ha proporcionado información sobre los riesgos y las estrategias para concientizar. También se encontró que nunca en un 100% se ha implementado estrategias para evaluar el riesgo que tienen los activos, la información y la cuantificación de los daños. Se tiene que un 97.5% a veces garantiza la seguridad. Así como a un 50% casi nunca se hace verificación de autenticidad de la información, trazabilidad, resolución de situaciones inesperadas.

Tabla 35.

Resultados de variable dependiente por cada una de sus dimensiones y sus indicadores en base al instrumento aplicado.

VARIABLES		Variable dependiente: Metodología Magerit V3							
DIMENSIONES	Dimensión 1: Cultura de riesgo de información		Dimensión 2: Gestión de riesgos			Dimensión 3: Infraestructura tecnológica		Dimensión 4: Recursos humanos	
INDICADORES	Personal capacitado	Personal concientizado	Nivel de planeación	Nivel de identificación	Nivel de valoración	Disponibilidad tecnológica	Conectividad	Nivel de pericia	Nivel de conocimiento
% X INDICADORES	21%	32%	10%	8%	8%	24%	40%	35%	33%
% X POR DIMENSION	27%		9%			32%		34%	
% X POR VARIABLE	25.5%								

Nota: Elaboración propia

Tabla 36.

Resultados de variable independiente por cada una de sus dimensiones y sus indicadores en base al instrumento aplicado.

VARIABLES		Variable Dependiente: Seguridad de la Información					
DIMENSIONES	Dimensión 1: Seguridad						
INDICADORES	Confidencialidad	Integridad	Disponibilidad	autenticidad	Trazabilidad	Disponibilidad	Disponibilidad
% X INDICADORES	40%	36%	40%	20%	20%	20%	37%
% X POR DIMENSION	30%						
% X POR VARIABLE	30%						

Nota: Elaboración propia

3.1.1. Análisis de normalidad

Con la finalidad de definir el estadístico a emplear en las pruebas de hipótesis, a continuación, se realizará la prueba de normalidad. Teniendo en cuenta que para esta prueba se admitirá la hipótesis alterna de normalidad que el p-valor sea menor 0.05 para pruebas no paramétricas y el p-valor mayor al 0.05 para pruebas paramétricas.

Tabla 37.

Prueba de normalidad

	Shapiro-Wilk		
	Estadístico	gL	Sig.
Metodología Magerit V3	.935	8	.561
Seguridad de la información	.798	8	.027

a. Corrección de significación de Lilliefors

Nota: Elaboración propia

Fue aplicada la prueba de normalidad de Shapiro-Wilk ya que se cuenta con una muestra pequeña (< 50). La prueba de normalidad se referencia en base a la hipótesis cuando los datos están ajustados a una distribución normal si la Sig. > 0,05 por consiguiente en la tabla puede contemplarse que para la variable Metodología Magerit V3 se cumple con esta hipótesis y se puede considerar que la misma proviene de una distribución normal con un nivel de confianza de 95%.

Respecto a la variable Seguridad de la Información, el valor de Sig. < 0,05 indica que la misma no se ajusta a la normalidad, descartándose la hipótesis estadística con un nivel de confianza de 95%. A partir de estos resultados se empleará la prueba de correlación no paramétrica Rho de Spearman para realizar las pruebas de hipótesis.

3.1.2. Prueba de hipótesis

A partir de los resultados obtenidos se procede a buscar la correlación de variables con la prueba de correlación no paramétrica Rho de Spearman ya que no se puede descartar que una de las variables presenta un comportamiento que se aleja de la normalidad.

Tabla 38.

Interpretación del coeficiente de correlación Rho de Spearman

-1.00	Correlación negativa perfecta
-0.90	Correlación negativa muy fuerte
-0.75	Correlación negativa considerable
-0.50	Correlación negativa media
-0.25	Correlación negativa débil
-0.10	Correlación negativa muy débil
0.00	No existe correlación alguna entre variables
+0.10	Correlación positiva muy débil
+0.25	Correlación positiva débil
+0.50	Correlación positiva media
+0.75	Correlación positiva considerable
+0.90	Correlación positiva muy fuerte
+1.00	Correlación positiva perfecta

Nota: Elaboración propia. Basado en (Hernández Sampieri, 1997)

a) Hipótesis

En base a la correlación de variables analizadas, se trazaron las hipótesis:

HG: La Metodología Magerit V3 influye de manera positiva en la seguridad de información de la empresa Deco Interiors SAC.

H₀: No Existe relación entre la Metodología Magerit V3 y la seguridad de información de la empresa Deco Interiors SAC.

H₁: Existe relación entre la Metodología Magerit V3 y la seguridad de información de la empresa Deco Interiors SAC.

Teniendo en cuenta que:

Sig. < 0.05, se rechaza la H_0 .

Sig. > 0.05, no se rechaza la H_0 .

Tabla 39.*Correlación entre las variables de la hipótesis general*

			Metodología Magerit V3	Seguridad de la Información
Rho de Spearman	Metodología Magerit V3	Coeficiente de correlación	1.00	.781*
		Sig. (2-tailed)		.022
		N	8	8
	Seguridad de la Información	Coeficiente de correlación	.781*	1.000
		Sig. (2-tailed)	.022	
		N	8	8

Nota: Elaboración propia

Análisis: la tabla 39 muestra los resultados que permiten deducir que la correlación entre la Metodología Magerit y la Seguridad de la Información a la muestra estadística de Spearman es de 0,781, esto muestra una correlación positiva importante entre las variables, de igual manera el valor de Sig.: $0,022 < 0,05$ indica que dicha correlación es estadísticamente significativa con un nivel de confianza de 95%, y permite refutar H_0 y aprobar la H_1 , a su vez se demuestra la hipótesis alterna como verdadera.

Tabla 40.*Resumen del modelo – Regresión Lineal y R2 (Metodología Magerit V3, Seguridad de la Información)*

Modelo	R	R cuadrado	R cuadrado ajustado	Error estándar de la estimación
1	.840 ^a	.706	.657	.436

a. Predictors: (constant), Metodología_Magerit_V3

Nota: Elaboración propia

Tabla 41.*Prueba de Anova, independiente y dependiente*

Modelo	Suma de cuadrados	gl	Media cuadrática	F	Sig.
1					
Regresión	2.735	1	2.735	14.391	.009 ^b
Residual	1.140	6	.190		
Total	3.875	7			

a. Variable dependiente: Seguridad de la información

b. Predictor: Metodología Magerit V3

Nota: Elaboración propia

Análisis: en la tabla 40 del resumen del modelo, se aprecia una correlación positiva importante de un 0.840 entre Metodología Magerit V3 y Seguridad de la Información. Asimismo, se establece que el 70,6% de la variación de la Seguridad de la información se debe a la influencia de la Metodología Magerit de acuerdo al coeficiente de determinación (R^2). La prueba Anova presentada en la tabla 41 evidencia que se obtuvo una significancia de $0.009 < 0.05$, lo que indica que el modelo lineal que relaciona las variables es significativo.

3.2. Discusión de resultados

El propósito principal de esta investigación es determinar la influencia de la Metodología Magerit V3 en la seguridad de la información de la empresa Deco Interiors SAC. A partir del análisis estadístico inferencial (prueba de correlación de Spearman) y regresión lineal con el propósito de cuantificar la causalidad que tiene la variable Metodología Magerit V3 sobre la seguridad de información de la referida compañía, como resultado se logró obtener una correlación positiva de gran consideración entre ellas con un nivel de significancia inferior a la propuesta en la investigación, así como lo indican (Hernández et. al., 2014). Los resultados también muestran una influencia superior al 70 por ciento de la variable Metodología Magerit V3 sobre la seguridad de la información, llegando a ser superior al 80 por ciento en ciertos casos, identificando de esta manera cuales son los puntos estratégicos donde

la empresa deberá establecer medidas de protección para el cuidado de la información.

Estos resultados concuerdan con los de Molina-Miranda (2017) quien en su estudio refirió que implementar la metodología Magerit permitirá a las empresas reconocer que es preciso poner en marcha un plan de gestión y tratamiento de riesgos que consienta atenuar los riesgos y establecer estrategias para disminuir las vulnerabilidades y amenazas a la que están sometidos los activos de información. Asimismo, agregó que toda empresa debe determinar y disminuir los riesgos de su información, pues si la compañía desconoce el peligro a los que se ven expuestos sus activos apenas podrá enfrentar si estos llegan a ocurrir. Por su parte Motaki (2016) luego de evaluar diversos métodos de análisis de riesgos señaló que el método Magerit V3 puede ser utilizado para determinar los riesgos y abre el camino para una certificación internacional cuando lo necesite la empresa, además, puede ser aplicada por unos pocos empleados cualificados.

3.3. Aporte práctico

3.3.1. Fundamentación del aporte práctico.

El proyecto se enfocó en determinar la influencia de la Metodología Magerit sobre la Seguridad de la Información con el propósito de evidenciar la necesidad de su aplicación sustentada en los resultados obtenidos en el presente proyecto. La empresa Deco Interiors SAC señaló no tener conocimiento de la existencia de estrategias que midan el nivel de riesgo al que se encuentran expuestos sus activos de información, así como las amenazas que pueden generar graves problemas llegando a interrumpir las labores diarias y hasta un desbalance económico en la empresa. Por esta razón el alcance de la investigación abarcó hasta la aplicación de un instrumento en el que se consultara a los empleados del departamento de informática sobre la seguridad de la información y las estrategias que hubiera llevado a cabo la empresa al respecto.

De acuerdo a los resultados obtenidos de la aplicación del cuestionario queda en evidencia que los empleados tienen el compromiso tanto con sus labores de trabajo como con la seguridad de la empresa y que ha sido una falta de estrategia por parte de la gerencia el hecho de no haber implementado una metodología para medir o identificar los riesgos informáticos, sin embargo, también señalaron que la empresa cuenta con políticas establecidas para asegurar la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información.

La aplicación de la metodología Magerit en la empresa Deco Interiors SAC le permitirá un mejor control tanto de la información que maneja como para la identificación de los riesgos y amenazas a los que se encuentra expuesta su información y lo más importante es que le permitirá establecer estrategias para solventar situaciones que se puedan presentar y evitar así daños mayores a la organización.

Una de las ventajas que tiene la metodología Magerit para la empresa es que cuenta con personal para llevar a cabo el proyecto sin tener que realizar una inversión considerable. Aunque no tienen conocimientos sólidos en el uso de este método, el nivel de complejidad no es elevado.

No obstante, deberán invertir en capacitación, mejorar la conectividad y actualizar algunos computadores de trabajo para aportar garantía en algunas tareas.

3.3.2. Construcción del aporte práctico

Sobre la base de los resultados del cuestionario y considerando el aporte teórico del marco descrito en capítulos previos, se propone la aplicación de la metodología Magerit en la empresa Deco Interiors SAC para disminuir peligros en lo que respecta a la implantación y utilización de las Tecnologías de la Información a través de la correspondiente estimación y análisis de los riesgos. Esta aplicación deberá considerar los siguientes pasos:

Obtener la EAR PILAR, es un software encargado del análisis y gestión de los riesgos bajo la metodología MAGERIT. Esta herramienta analiza los riesgos considerando las dimensiones de la seguridad de la información.

Los resultados que arroja son tratados a partir de: salvaguardas, pautas y operaciones de seguridad.

Las etapas que contempla son:

- Caracterización de los activos: identificación, clasificación, dependencias y valoración.
- Caracterización de las amenazas.
- Evaluación de las salvaguardas.
- Proceso de Gestión de riesgos.
- Plan de tratamiento de los riesgos.

Los resultados de dicha herramienta mostrarán los gráficos que reflejarán los niveles de riesgo e impacto potencial, actual y objetivo. Con estos resultados se deberán realizar acciones para concientizar a los empleados respecto a la seguridad de la información, así como a implementar normas que los empleados deberán seguir para lograr un control de la información en la empresa.

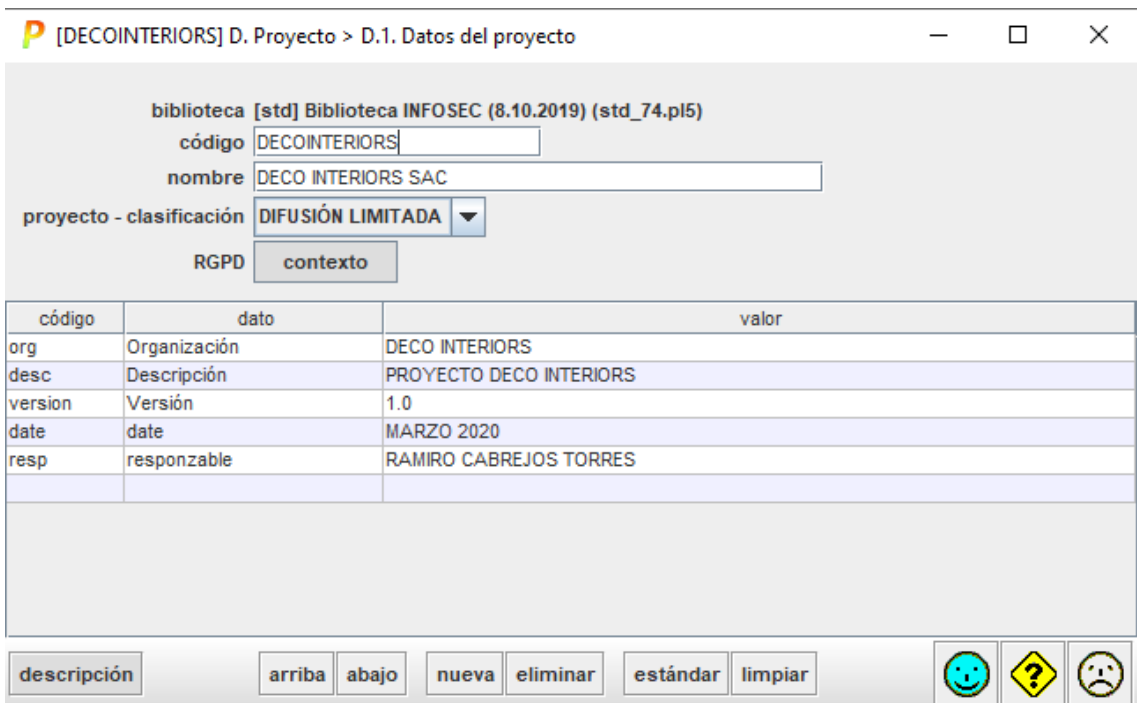
Aplicación de la herramienta PILAR bajo la Metodología Magerit según las etapas mencionadas.

3.3.3. Creación del proyecto en PILAR

En base a la estructura planteada por la metodología Magerit V3, se ha definido la estructura de la empresa Deco Interiors para realizar un análisis cualitativo en la herramienta PILAR 7.4.2 en modo evaluación, la cual permitirá clasificar la información que se ha propuesto en la investigación y de esta manera lograr un análisis y gestionar los riesgos de la empresa Deco Interiors a través de la caracterización de los activos, caracterización de las amenazas.

Figura 28.

Datos del Proyecto



The screenshot shows the 'Datos del proyecto' window in the PILAR software. The window title is '[DECOINTERIORS] D. Proyecto > D.1. Datos del proyecto'. The interface includes several input fields and a table:

- biblioteca**: [std] Biblioteca INFOSEC (8.10.2019) (std_74.pl5)
- código**: DECOINTERIORS
- nombre**: DECO INTERIORS SAC
- proyecto - clasificación**: DIFUSIÓN LIMITADA (dropdown menu)
- RGPD**: contexto (button)

código	dato	valor
org	Organización	DECO INTERIORS
desc	Descripción	PROYECTO DECO INTERIORS
version	Versión	1.0
date	date	MARZO 2020
resp	responsable	RAMIRO CABREJOS TORRES

At the bottom of the window, there are several buttons: descripción, arriba, abajo, nueva, eliminar, estándar, limpiar, and three icons (smiley face, question mark, sad face).

Nota: Elaboración propia. Software PILAR 7.4.2

3.3.4. Caracterización de los activos

Esta actividad consta de tres actividades la identificación de los activos, las dependencias y su valoración.

El objetivo es reconocer en el sistema a analizar, los activos más importantes que lo componen, se caracteriza por el tipo de activo y se identifica las relaciones entre ellos, definiendo en que dimensiones de seguridad son importantes y se valora su importancia.

3.3.4.1 Identificación de Activos

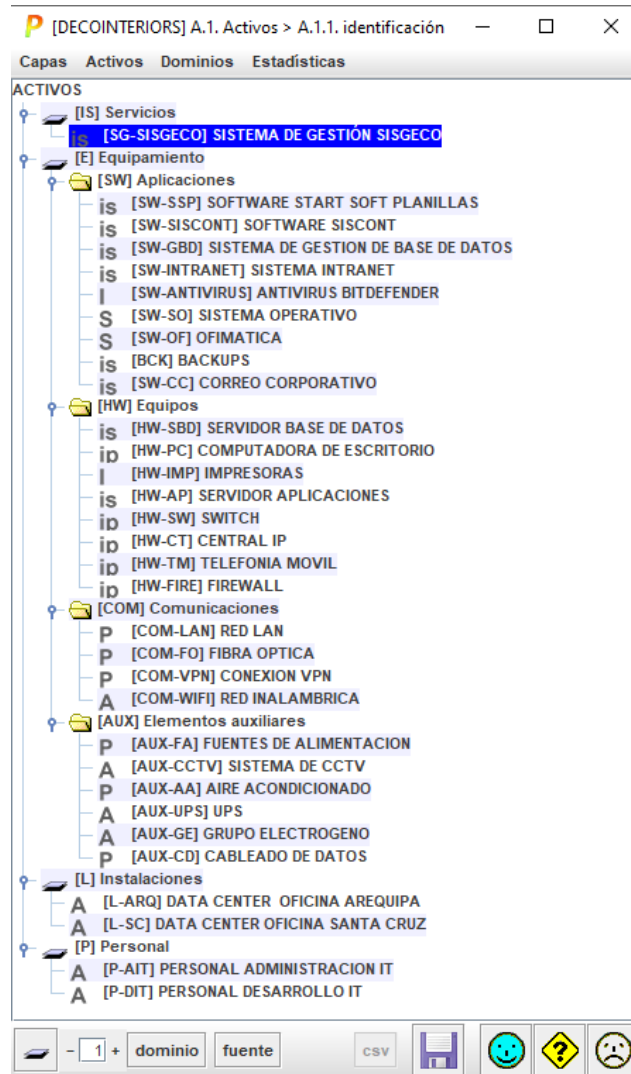
Los activos son aquellos componentes o funcionalidad del Sistema de Información sensible a ser atacado de manera deliberada o accidentalmente con repercusiones en la organización. En un Sistema de Información has 02 cosas esenciales: La información que maneja y los servicios que presta en ese sentido la GSI de la empresa Deco Interiors es organizada a través de sus activos y recursos que generan, procesan, almacenan y transmiten información de valor a la empresa. En la siguiente tabla se listan por capa cada uno de los activos con la debida descripción de cada uno de ellos.

Véase ANEXO 6 Tabla 66 Identificación de activos

Se utilizó el la herramienta PILAR 7.4.2 en el proceso de identificación de activos para registrar los datos de cada uno.

Figura 29.

Identificación de activos



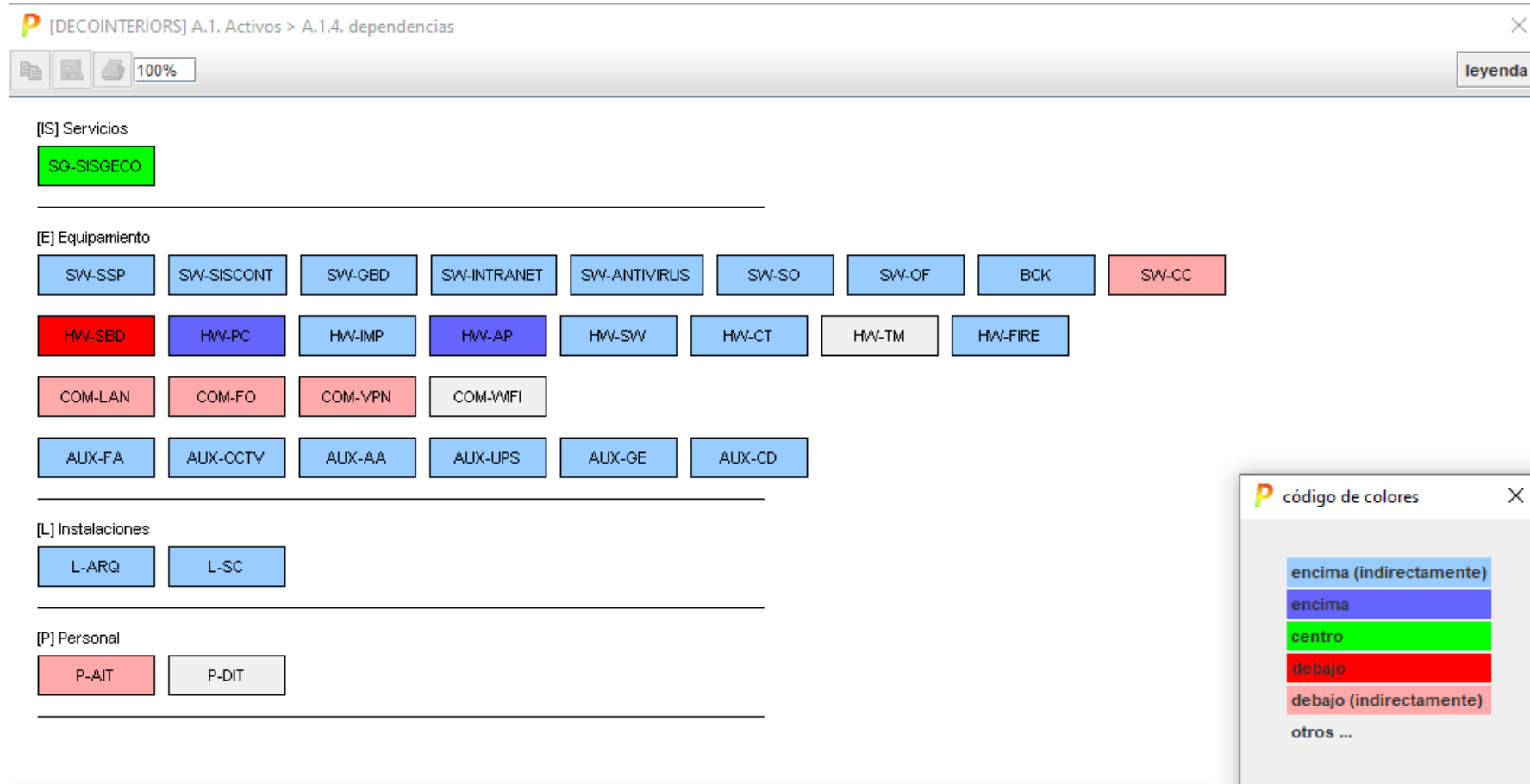
Nota: Elaboración propia. Software PILAR 7.4.2

3.3.4.2 Dependencia entre activos

En el presente gráfico se puede reflejar desde la parte superior hacia la inferior las dependencias, mientras que de la parte inferior hacia la superior la propagación del daño en caso de materializarse la amenaza. En la gráfica se muestra la dependencia que existe entre los activos, teniendo al Sistema de Gestión Sisgeco como el activo superior más valioso para la organización frente a una amenaza y depende de los activos que se encuentran más abajo a diferencia de un activo de orden inferior los cuales soportan el valor por delegación.

Figura 30.

Dependencia entre activos



Nota: Elaboración propia. Software PILAR 7.4.2

3.3.4.3 Valoración de activos

El objetivo principal de esta tarea es ver desde la perspectiva de la necesidad de proteger ya que cuanto más valioso es un activo, mayor nivel de protección requiere en la dimensión(es) de seguridad que sea pertinente. Su valor puede ser propio o acumulado. Para este caso los activos inferiores en un esquema de dependencia, acumulan el valor de los activos que se apoyan de ellos.

Para la investigación se ha identificado en qué dimensión es valioso el activo, para el funcionamiento adecuado de los procesos de la organización, para ello fue necesario definir atributos para valorar los activos en términos de su importancia y las consecuencias que se puedan desencadenar en caso que estos se vean comprometidos bajo una amenaza.

Para la valoración de activos Magerit presenta una escala en la que se establecen criterios para identificar las dimensiones en la que el activo es relevante.

Tabla 42.

Criterios de valoración de activos

VALOR	NIVEL	CRITERIOS
10	Nivel 10	Extremo
9	Nivel 9	Muy alto
8	Nivel 8 (+)	
7	Alto	Alto
6	Alto (-)	
5	Medio (+)	
4	Medio	Medio
3	Medio (-)	
2	Bajo (+)	
1	Bajo	Bajo
0	Despreciable	Despreciable

Nota: Elaboración propia. Tomado de Libro II Catálogo de elementos, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (Administración Electrónica, 2012)

Tabla 43.

Dimensiones de la valoración de activos

CÓDIGO	DIMENSIÓN
[D]	Disponibilidad
[I]	Integridad de los datos
[C]	Confidencialidad de los datos Autenticidad de los usuarios y de la información
[A]	
[T]	Trazabilidad del servicio y de los datos

Nota: Elaboración propia. Tomado de Libro II Catálogo de elementos, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (Administración Electrónica, 2012)

Véase ANEXO 7 Tabla 67 Valoración de activos

A través del Sistema PILAR se registró la valoración de cada uno de los activos que tienen por atributos.

Figura 31.

Valoración propia de los activos

[DECOINTERIORS] A.1. Activos > A.1.5. valoración de los activos

Editar Exportar Importar

activo	[D]	[I]	[C]	[A]	[T]
ACTIVOS					
[IS] Servicios					
[SG-SISGECO] SISTEMA DE GESTIÓN SISGECO	[10]	[9]	[10]	[10]	[9]
[E] Equipamiento					
[SW] Aplicaciones					
is [SW-SSP] SOFTWARE START SOFT PLANILLAS	[8]	[8]	[9]	[9]	[8]
is [SW-SISCONT] SOFTWARE SISCONT	[9]	[8]	[8]	[8]	[7]
is [SW-GBD] SISTEMA DE GESTION DE BASE DE DATOS	[10]	[9]	[9]	[8]	[7]
is [SW-INTRANET] SISTEMA INTRANET	[7]	[7]	[7]	[6]	[6]
I [SW-ANTIVIRUS] ANTIVIRUS BITDEFENDER	[8]	[5]	[5]	[5]	[5]
S [SW-SO] SISTEMA OPERATIVO	[6]		[1]	[5]	[1]
S [SW-OF] OFIMATICA	[5]	[3]			
is [BCK] BACKUPS	[10]	[9]	[8]	[9]	[7]
is [SW-CC] CORREO CORPORATIVO	[9]	[8]	[8]	[9]	[7]
[HW] Equipos					
is [HW-SBD] SERVIDOR BASE DE DATOS	[10]	[9]	[9]	[8]	[8]
ip [HW-PC] COMPUTADORA DE ESCRITORIO	[9]	[7]	[7]	[8]	
I [HW-IMP] IMPRESORAS	[7]		[7]	[7]	
is [HW-AP] SERVIDOR APLICACIONES	[10]	[9]	[9]	[9]	[8]
ip [HW-SW] SWITCH	[9]				
ip [HW-CT] CENTRAL IP	[9]	[8]	[7]	[8]	
ip [HW-TM] TELEFONIA MOVIL	[8]	[8]	[7]	[8]	
ip [HW-FIRE] FIREWALL	[10]				
[COM] Comunicaciones					
P [COM-LAN] RED LAN	[9]	[9]	[9]	[9]	
P [COM-FO] FIBRA OPTICA	[10]	[9]	[9]	[9]	
P [COM-VPN] CONEXION VPN	[9]	[9]	[9]	[9]	
A [COM-WIFI] RED INALAMBRICA	[7]			[9]	
[AUX] Elementos auxiliares					
P [AUX-FA] FUENTES DE ALIMENTACION	[6]				
A [AUX-CCTV] SISTEMA DE CCTV	[7]		[8]	[8]	
P [AUX-AA] AIRE ACONDICIONADO	[8]				
A [AUX-UPS] UPS	[9]				
A [AUX-GE] GRUPO ELECTROGENO	[8]				
P [AUX-CD] CABLEADO DE DATOS	[8]				
[L] Instalaciones					
A [L-ARQ] DATA CENTER OFICINA AREQUIPA	[9]	[8]	[8]	[8]	
A [L-SC] DATA CENTER OFICINA SANTA CRUZ	[9]	[8]	[8]	[8]	
[P] Personal					
A [P-AIT] PERSONAL ADMINISTRACION IT	[9]	[8]	[8]	[8]	
A [P-DIT] PERSONAL DESARROLLO IT	[8]	[6]	[8]	[6]	

origenes valor acumulado marca

Nota: Elaboración propia. Software PILAR 7.4.2

3.3.5. Caracterización de las amenazas

En esta tarea el objetivo es poder reconocer las amenazas más importantes a las que se enfrenta el sistema a analizar, caracterizándolas por las estimaciones de ocurrencia o probabilidad y daño causado o degradación.

3.3.5.1 Identificación de amenazas

Se debe identificar, determinar y conocer toda amenaza a la que se enfrentan los activos, además de la probabilidad de que esta pueda ocurrir y la degradación que éstas causan sobre el valor de los activos.

Identificar las amenazas que puedan poner en riesgo los activos, las amenazas están clasificadas en cinco grupos:

Tabla 44.

Identificación de amenazas

CÓDIGO	IDENTIFICACIÓN DE AMENAZAS
[N]	Desastres naturales
[I]	De origen industrial
[E]	Errores y fallos no intencionados
[A]	Ataques deliberados
[PR]	Riesgos de privacidad

Nota: Elaboración propia. Tomado de Libro II Catálogo de elementos, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (Administración Electrónica, 2012)

Como se puede observar en la imagen las amenazas identificadas se encuentran registrados en PILAR, para poder hacer las estimaciones de ocurrencia en cuanto a probabilidad y la degradación ocasionado por el daño que podría causar

Véase ANEXO 08 Tabla 68 Identificación de amenazas

Figura 32. Identificación de amenazas en cada uno de los activos

The screenshot displays the PILAR 7.4.2 software interface for identifying threats. The left pane, titled 'ACTIVOS', shows a tree view of assets categorized into: [IS] Servicios, [E] Equipamiento, [SW] Aplicaciones, [HW] Equipos, [COM] Comunicaciones, [AUX] Elementos auxiliares, [L] Instalaciones, and [P] Personal. The right pane, titled 'AMENAZAS', lists various threats such as [N] Desastres naturales, [E] Errores y fallos no intencionados, and [A] Ataques deliberados, each with a red triangle icon. The interface includes a top menu bar, a toolbar with 'aplicar' and 'eliminar' buttons, and a status bar with icons for help, warning, and error.

Nota: Elaboración propia. Software PILAR 7.4.2

3.3.5.2 Valoración de amenazas

El objetivo es identificar las amenazas y estimar la frecuencia de ocurrencia sobre cada activo, estimando la degradación que causaría la amenaza en cada dimensión del activo si llegara a materializarse y la probabilidad. El resultado de esta actividad es el informe denominado “mapa de riesgos”.

Para evaluar la probabilidad de ocurrencia de cada amenaza, se tendrá en cuenta los siguientes criterios:

Tabla 45.

Probabilidad de Ocurrencia

VALOR CUALITATIVO	FRECUENCIA	DESCRIPCIÓN
CS	A diario	Casi seguro
MA	Cada semana	Muy alto
P	Cada mes	Posible
PP	Cada año	Poco probable
MB	Cada varios años	Muy baja
MR	Cada siglo	Muy raro

Nota: Elaboración propia. Tomado de Libro III Guía de técnicas (Administración Electrónica, 2012)

Tabla 46.

Degradación del activo

PROBABILIDAD DE OCURRENCIA	
MA	Muy alto
A	Alto
M	Moderado
B	Bajo
MB	Muy bajo

Nota: Elaboración propia. Tomado de Libro III Guía de técnicas (Administración Electrónica, 2012)

Véase ANEXO 09 Tabla 69 Valoración de las amenazas.

Figura 33.

Valoración de las amenazas sobre los activos

activo	co...	probabilidad	[D]	[I]	[C]	[A]	[T]
ACTIVOS							
[IS] Servicios							
[SG-SISGECO] SISTEMA DE GESTIÓN SISGECO			10%	10%	10%	10%	10%
[E.15] Avería de origen físico o lógico		P	5%				
[E.1] Errores de los usuarios		P	1%	1%	1%		
[E.2] Errores del administrador del sistema / de la		P	2%	2%	2%		
[E.8] Difusión de software dañino		P	1%	1%	1%		
[E.15] Alteración de la información		P		1%			
[E.18] Destrucción de la información		P	1%				
[E.19] Fugas de información		P			1%		
[E.20] Vulnerabilidades de los programas (softwa		P	0	2%	2%		
[E.24] Caída del sistema por agotamiento de recur		MA	5%				
[E.28] Indisponibilidad del personal		P	2%				
[A.5] Suplantación de la identidad		CS		5%	5%	10%	
[A.6] Abuso de privilegios de acceso		CS	0	1%	5%	10%	
[A.7] Uso no previsto		MA	0	1%	1%		
[A.8] Difusión de software dañino		MA	10%	10%	10%		
[A.11] Acceso no autorizado		CS		1%	5%	10%	
[A.13] Repudio (negación de actuaciones)		MA					10%
[A.15] Modificación de la información		CS		5%			
[A.18] Destrucción de la información		MA	5%				
[A.19] Revelación de información		CS			5%		
[A.22] Manipulación de programas		MA	5%	10%	10%		
[A.24] Denegación de servicio		CS	5%				
[A.28] Indisponibilidad del personal		P	5%				
[A.29] Extorsión		MA	5%	10%	10%		
[A.30] Ingeniería social (picaresca)		P	5%	10%	10%		
[E] Equipamiento							
[SW] Aplicaciones							
[SW-SSP] SOFTWARE START SOFT PLANILLAS			10%	10%	10%	10%	10%
[SW-SISCONT] SOFTWARE SISCONT			10%	10%	10%	10%	10%
[SW-GBD] SISTEMA DE GESTION DE BASE DE DATOS			10%	10%	10%	10%	10%
[SW-INTRANET] SISTEMA INTRANET			10%	10%	10%	10%	10%
[SW-ANTIVIRUS] ANTIVIRUS BITDEFENDER			10%	10%	10%		
[SW-SO] SISTEMA OPERATIVO			10%	10%	10%	10%	10%
[SW-OF] OFIMATICA			1%	10%	10%		
[BCK] BACKUPS			10%	10%	10%	10%	10%
[SW-CC] CORREO CORPORATIVO			10%	10%	10%	10%	10%
[HW] Equipos							
[HW-SBD] SERVIDOR BASE DE DATOS			10%	10%	10%	10%	
[HW-PC] COMPUTADORA DE ESCRITORIO			10%	10%	10%	10%	10%
[HW-IMP] IMPRESORAS			10%		5%	10%	
[HW-AP] SERVIDOR APLICACIONES			10%	10%	10%	10%	
[HW-SW] SWITCH			10%	5%	5%		
[HW-CT] CENTRAL IP			10%	5%	5%	10%	10%
[HW-TM] TELEFONIA MOVIL			10%	5%	5%	10%	
[HW-FIRE] FIREWALL			10%	5%	5%		
[COM] Comunicaciones							
[COM-LAN] RED LAN			5%	5%	5%	10%	
[COM-FO] FIBRA OPTICA			10%	10%	10%	10%	10%
[COM-VPN] CONEXION VPN			10%	10%	10%	10%	10%
[COM-WIFI] RED INALAMBRICA			5%			10%	
[AUX] Elementos auxiliares							
[AUX-FA] FUENTES DE ALIMENTACION			10%				
[AUX-CCTV] SISTEMA DE CCTV			10%	10%	10%		
[AUX-AA] AIRE ACONDICIONADO			5%				
[AUX-UPS] UPS			5%				
[AUX-GE] GRUPO ELECTROGENO			5%				

Nota: Elaboración propia. Software PILAR 7.4.2

3.3.6. Caracterización de las Salvaguardas

El objetivo de esta tareas es saber qué necesitamos realizar para proteger el sistema y saber si tenemos un sistema de protección a la altura de nuestras necesidades.

3.3.6.1 Identificación y valoración de las Salvaguardas

MAGERIT define a las salvaguardas o contra medidas como mecanismos y procedimientos que mitiguen los riesgos a los que se enfrenta la organización.

Tabla 47.

Aspecto de las salvaguardas

ASPECTO	
G	Para gestión
T	Para técnico
F	Para seguridad física
P	Para gestión de personal

Nota: Elaboración propia. Tomado de Libro III Guía de técnicas (Administración Electrónica, 2012)

Tabla 48.

Tipo de protección

TIPO DE PROTECCIÓN	
PR	Prevención
EL	Eliminación
CR	Corrección
MN	Monitorización
RC	Recuperación

Nota: Elaboración propia. Tomado de Libro III Guía de técnicas (Administración Electrónica, 2012)

Tabla 49.*Pesos relativos*

PESOS RELATIVOS	
máximo peso	crítica
peso alto	muy importante
peso normal	importante
peso bajo	interesante
<u>aseguramiento: componentes certificados</u>	

Nota: Elaboración propia. Tomado de Libro III Guía de técnicas (Administración Electrónica, 2012)

Se registra en PILAR los valores que se realizaron en la etapa anterior, de esta manera podremos ver los riesgos e impacto que las amenazas generan y el objetivo al que deseamos llegar para mitigarlas.

Tabla 50.*Nivel de madurez*

NIVEL	MADUREZ	ESTADO
L0	inexistente	inexistente
L1	inicial/ad hoc reproducibile, pero	iniciado parcialmente
L2	intuitivo	realizado
L3	proceso definido	en funcionamiento
L4	gestionado y medible	monitorizando
L5	optimizado	mejora continua

Nota: Elaboración propia. Tomado de Libro III Guía de técnicas (Administración Electrónica, 2012)

Véase ANEXO 10 Tabla 70 Identificación y valoración de las Salvaguardas

Figura 34.

Identificación y valoración de las salvaguardas

asp...	tdp	rec...	salvaguarda	dudas	fuelle	aplica	comen...	corre...	target	PILAR
			SALVAGUARDAS					_-L2	_-L4	L2-L5
	G	EL	8					L0-L2	L3-L4	L2-L5
	G	std	3					L1	L4	L3
	G	proc	3					L1	L4	L3
	G	EL	5					L2	L4	L3
	G	EL	5					L2	L4	L3
	G	EL	3					L2	L4	L3
	T	EL	3					L2	L4	L3
	G	EL	5					L0	L3	L2-L3
	G	AD	2					L0	L3	L2
	G	AD	5					L0	L3	L2-L3
	G	EL	4					L0	L3	L3
	G	EL	3					L0	L3	L3
	G	EL	3					L0	L3	L3
	G	AD	2					L0	L3	L2
	G	AD	2					L0	L3	L2
	G	AD	2					L0	L3	L2
	G	AD	2					L0	L3	L2
	G	MN	2					L0	L3	L2
	G	IM	5					L0	L3	L3
	G	EL	5					L0	L3	L2-L3
	T	EL	7					L0	L4	L4
	G	PR	8					L0	L4	L4-L5
	T	EL	7					L1	L4	L2-L4
	G	PR	8					L1	L4	L2-L5
	G	EL								n.a.
	G	PR	6					L1	L4	L2-L4
	G	PR	7					L1	L4	L2-L4
	G	PR	7					L1	L4	L2-L4
	G	PR	8					L1	L4	L2-L5
	G	PR								n.a.
	G	PR	7					L1	L1	L2-L4
	G	PR	6					L1	L4	L2-L4
	F	EL	6					L2	L4	L3-L4
	F	PR	7					L2	L4	L2-L4
	F	EL								n.a.
	P	PR	6					L1	L4	L2-L4
	G	PR						L2	L2	n.a.
	G	CR	6					L0	L4	L2-L4

Nota: Elaboración propia. Software PILAR 7.4.2

En la figura se observa la columna recomendación, en la cual se tiene en cuenta el activo con una valoración de la salvaguardia de 0 a 10, en las columnas posteriores se registra el presente nivel de madurez de salvaguardas, en la siguiente columna el objetivo que hemos propuesto y finalmente el nivel recomendado por la EAR PILAR.

3.3.7. Estimación del Estado de Riesgo

Esta actividad involucra estimar el impacto y el riesgo. La estimación del estado de riesgo se ha calculado automáticamente en la EAR PILAR, la cual es el resultado del vínculo de la probabilidad de que el riesgo suceda y el impacto producido por la ocurrencia del riesgo.

3.3.7.1 Estimación del Riesgo

En esta actividad estimamos el riesgo al cual se somete el sistema, a través del riesgo potencial y riesgo residual

3.3.7.1.1 Riesgo Potencial

En la siguiente figura 35 se puede identificar el riesgo al que es enfrentado cada activo, podemos identificar por los colores el nivel de criticidad, podemos identificar que el nivel de riesgo del sistema que está siendo evaluado es crítico, por lo que es necesario implementar las salvaguardas de manera inmediata para mitigar los riesgos.

Véase ANEXO 11 Tabla 71 Riesgo potencial de los activos

Figura 35.

Riesgo potencial de los activos

potencial		current	target	PILAR				
activo		[D]	[I]	[C]	[A]	[T]		
<input type="checkbox"/>	ACTIVOS	{6,7}	{6,7}	{7,0}	{7,6}	{5,7}		
<input type="checkbox"/>	[IS] Servicios	{6,1}	{5,6}	{7,0}	{7,6}	{5,7}		
<input type="checkbox"/>	is [SG-SISGECO] SISTEMA DE GESTIÓN SISGECO	{6,1}	{5,6}	{7,0}	{7,6}	{5,7}		
<input type="checkbox"/>	[E] Equipamiento	{6,7}	{6,7}	{7,0}	{7,6}	{5,7}		
<input type="checkbox"/>	[SW] Aplicaciones	{6,7}	{6,7}	{7,0}	{7,6}	{5,7}		
<input type="checkbox"/>	is [SW-SSP] SOFTWARE START SOFT PLANILLAS	{6,1}	{6,2}	{7,0}	{7,6}	{5,7}		
<input type="checkbox"/>	is [SW-SISCONT] SOFTWARE SISCONT	{6,1}	{6,2}	{7,0}	{7,6}	{5,7}		
<input type="checkbox"/>	is [SW-GBD] SISTEMA DE GESTION DE BASE DE DATOS	{6,1}	{6,2}	{6,2}	{5,8}	{5,7}		
<input type="checkbox"/>	is [SW-INTRANET] SISTEMA INTRANET	{4,4}	{4,4}	{4,4}	{4,0}	{3,9}		
<input type="checkbox"/>	I [SW-ANTIVIRUS] ANTIVIRUS BITDEFENDER	{5,8}	{5,8}	{6,2}				
<input type="checkbox"/>	S [SW-SO] SISTEMA OPERATIVO	{6,1}	{6,2}	{6,2}	{5,8}	{5,7}		
<input type="checkbox"/>	S [SW-OF] OFIMATICA	{4,0}	{5,8}	{6,2}				
<input type="checkbox"/>	is [BCK] BACKUPS	{6,7}	{6,7}	{7,0}	{7,6}	{5,7}		
<input type="checkbox"/>	is [SW-CC] CORREO CORPORATIVO	{5,8}	{6,7}	{7,0}	{6,7}	{5,0}		
<input type="checkbox"/>	[HW] Equipos	{6,7}	{6,2}	{7,0}	{7,6}	{5,7}		
<input type="checkbox"/>	is [HW-SBD] SERVIDOR BASE DE DATOS	{6,0}	{5,8}	{7,0}	{6,7}			
<input type="checkbox"/>	id [HW-PC] COMPUTADORA DE ESCRITORIO	{6,7}	{6,2}	{7,0}	{7,6}	{5,7}		
<input type="checkbox"/>	I [HW-IMP] IMPRESORAS	{4,9}		{5,3}	{5,8}			
<input type="checkbox"/>	is [HW-AP] SERVIDOR APLICACIONES	{6,0}	{5,8}	{7,0}	{6,7}			
<input type="checkbox"/>	id [HW-SW] SWITCH	{6,0}	{5,3}	{5,5}				
<input type="checkbox"/>	id [HW-CT] CENTRAL IP	{6,7}	{6,2}	{5,5}	{5,8}	{5,7}		
<input type="checkbox"/>	id [HW-TM] TELEFONIA MOVIL	{5,5}	{5,0}	{3,7}	{4,6}			
<input type="checkbox"/>	id [HW-FIRE] FIREWALL	{6,0}	{5,3}	{5,5}				
<input type="checkbox"/>	[COM] Comunicaciones	{6,1}	{5,8}	{6,2}	{5,8}	{5,0}		
<input type="checkbox"/>	P [COM-LAN] RED LAN	{6,1}	{5,3}	{5,5}	{5,8}			
<input type="checkbox"/>	P [COM-FO] FIBRA OPTICA	{6,1}	{5,8}	{6,2}	{5,8}	{5,0}		
<input type="checkbox"/>	P [COM-VPN] CONEXION VPN	{6,1}	{5,8}	{6,2}	{5,8}	{5,0}		
<input type="checkbox"/>	A [COM-WIFI] RED INALAMBRICA	{4,4}			{5,2}			
<input type="checkbox"/>	[AUX] Elementos auxiliares	{5,2}	{5,6}	{6,2}				
<input type="checkbox"/>	P [AUX-FA] FUENTES DE ALIMENTACION	{3,3}						
<input type="checkbox"/>	A [AUX-CCTV] SISTEMA DE CCTV	{5,2}	{5,6}	{6,2}				
<input type="checkbox"/>	P [AUX-AA] AIRE ACONDICIONADO	{3,9}						
<input type="checkbox"/>	A [AUX-UPS] UPS	{4,2}						
<input type="checkbox"/>	A [AUX-GE] GRUPO ELECTROGENO	{3,6}						
<input type="checkbox"/>	P [AUX-CD] CABLEADO DE DATOS	{4,5}						
<input type="checkbox"/>	[L] Instalaciones	{5,6}	{5,6}	{6,2}				
<input type="checkbox"/>	A [L-ARQ] DATA CENTER OFICINA AREQUIPA	{5,6}	{5,6}	{6,2}				
<input type="checkbox"/>	A [L-SC] DATA CENTER OFICINA SANTA CRUZ	{5,6}	{5,6}	{6,2}				
<input type="checkbox"/>	[P] Personal	{5,1}	{5,8}	{7,0}	{6,7}			
<input type="checkbox"/>	A [P-AIT] PERSONAL ADMINISTRACION IT	{5,1}	{5,8}	{7,0}	{6,7}			
<input type="checkbox"/>	A [P-DIT] PERSONAL DESARROLLO IT	{3,9}	{3,5}	{5,9}	{4,3}			

P niveles de criticidad

- (9) - catástrofe
- (8) - desastre
- (7) - extremadamente crítico
- (6) - muy crítico
- (5) - crítico
- (4) - muy alto
- (3) - alto
- (2) - medio
- (1) - bajo
- (0) - despreciable

leyenda

Nota: Elaboración propia. Software PILAR 7.4.2

3.3.7.1.2 Riesgo Residual

Los resultados del riesgo residual son facilitados por la EAR PILAR, estos riesgos residuales se muestran a pesar de haber desplegado un conjunto de salvaguardas alcanzando un nivel de maduración.

Véase ANEXO 12 Tabla 72 Riesgo residual de los activos

Figura 36.

Riesgo residual de los activos

[DECOINTERIORS] A.6.2. Valores acumulados > A.6.2.2. riesgo

Ver Exportar

potencial current target **PILAR**

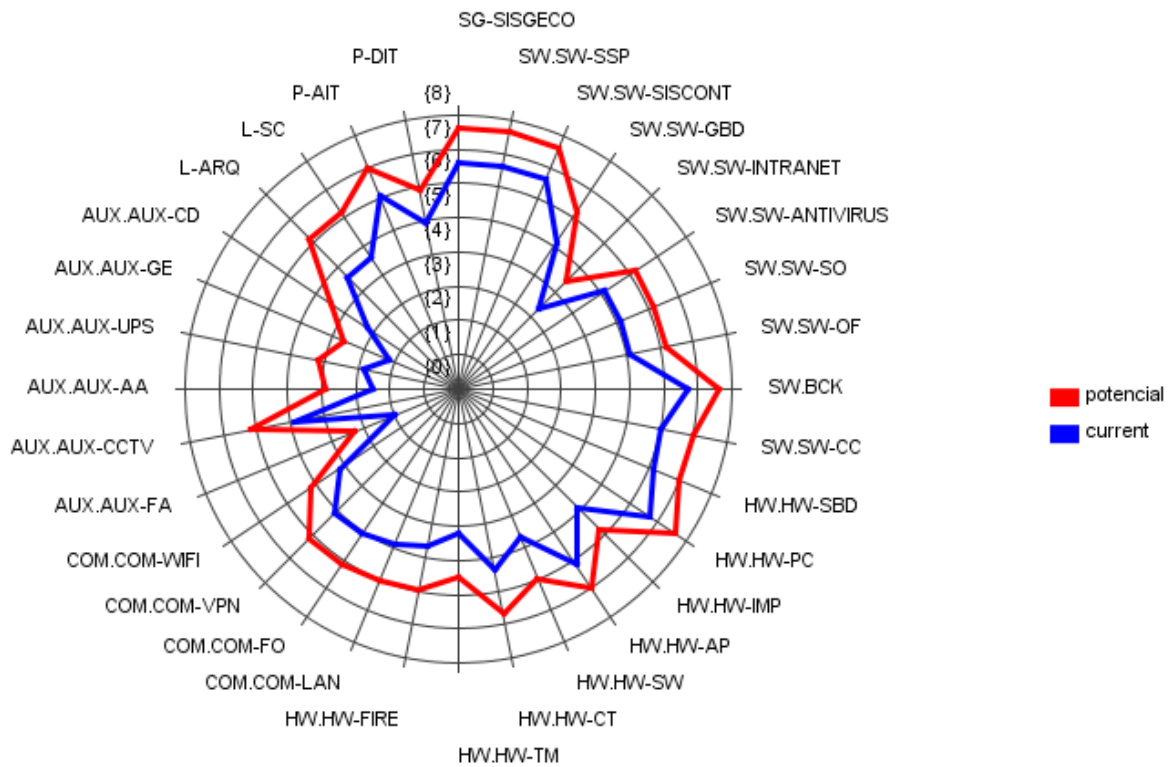
activo	[D]	[I]	[C]	[A]	[T]
ACTIVOS	{2,7}	{2,7}	{3,2}	{3,5}	{1,8}
[IS] Servicios	{1,9}	{1,3}	{2,7}	{3,3}	{1,6}
is [SG-SISGECO] SISTEMA DE GESTIÓN SISGECO	{1,9}	{1,3}	{2,7}	{3,3}	{1,6}
[E] Equipamiento	{2,7}	{2,7}	{3,0}	{3,5}	{1,8}
[SW] Aplicaciones	{2,7}	{2,7}	{3,0}	{3,5}	{1,8}
is [SW-SSP] SOFTWARE START SOFT PLANILLAS	{1,9}	{1,9}	{2,7}	{3,3}	{1,6}
is [SW-SISCONT] SOFTWARE SISCONT	{1,9}	{1,9}	{2,7}	{3,3}	{1,6}
is [SW-GBD] SISTEMA DE GESTION DE BASE DE DATOS	{1,9}	{1,8}	{1,8}	{1,7}	{1,5}
is [SW-INTRANET] SISTEMA INTRANET	{0,82}	{0,81}	{0,81}	{0,78}	{0,74}
I [SW-ANTIVIRUS] ANTIVIRUS BITDEFENDER	{1,5}	{1,5}	{1,8}		
S [SW-SO] SISTEMA OPERATIVO	{1,9}	{1,8}	{1,8}	{1,7}	{1,5}
S [SW-OF] OFIMATICA	{0,74}	{1,5}	{1,8}		
is [BCK] BACKUPS	{2,7}	{2,7}	{3,0}	{3,5}	{1,8}
is [SW-CC] CORREO CORPORATIVO	{1,6}	{2,4}	{2,8}	{2,5}	{0,98}
[HW] Equipos	{2,7}	{2,2}	{3,0}	{3,5}	{1,8}
is [HW-SBD] SERVIDOR BASE DE DATOS	{2,0}	{1,8}	{3,0}	{2,7}	
id [HW-PC] COMPUTADORA DE ESCRITORIO	{2,7}	{2,2}	{3,0}	{3,5}	{1,8}
I [HW-IMP] IMPRESORAS	{0,98}		{1,2}	{1,7}	
is [HW-AP] SERVIDOR APLICACIONES	{2,0}	{1,8}	{3,0}	{2,7}	
id [HW-SW] SWITCH	{2,0}	{1,2}	{1,4}		
id [HW-CT] CENTRAL IP	{2,7}	{2,1}	{1,4}	{1,8}	{1,7}
id [HW-TM] TELEFONIA MOVIL	{1,5}	{0,98}	{0,72}	{0,92}	
id [HW-FIRE] FIREWALL	{2,0}	{1,2}	{1,4}		
[COM] Comunicaciones	{2,3}	{2,0}	{2,3}	{2,1}	{1,1}
P [COM-LAN] RED LAN	{2,3}	{1,3}	{1,5}	{2,0}	
P [COM-FO] FIBRA OPTICA	{2,3}	{2,0}	{2,3}	{2,1}	{1,1}
P [COM-VPN] CONEXION VPN	{2,3}	{2,0}	{2,3}	{2,1}	{1,1}
A [COM-WIFI] RED INALAMBRICA	{0,89}			{1,4}	
[AUX] Elementos auxiliares	{1,4}	{1,7}	{2,3}		
P [AUX-FA] FUENTES DE ALIMENTACION	{0,70}				
A [AUX-CCTV] SISTEMA DE CCTV	{1,4}	{1,7}	{2,3}		
P [AUX-AA] AIRE ACONDICIONADO	{0,80}				
A [AUX-UPS] UPS	{0,86}				
A [AUX-GE] GRUPO ELECTROGENO	{0,74}				
P [AUX-CD] CABLEADO DE DATOS	{0,94}				
[L] Instalaciones	{1,9}	{1,8}	{2,3}		
A [L-ARQ] DATA CENTER OFICINA AREQUIPA	{1,9}	{1,8}	{2,3}		
A [L-SC] DATA CENTER OFICINA SANTA CRUZ	{1,9}	{1,8}	{2,3}		
[P] Personal	{1,2}	{1,9}	{3,2}	{2,8}	
A [P-AIT] PERSONAL ADMINISTRACION IT	{1,2}	{1,9}	{3,2}	{2,8}	
A [P-DIT] PERSONAL DESARROLLO IT	{0,81}	{0,72}	{2,0}	{0,88}	

- 1 + +1 dominio fuente gestionar leyenda

Nota: Elaboración propia. Software PILAR 7.4.2. Lo que se muestra en la figura 37, son los resultados del análisis de riesgos a las que quedan expuestos la organización, la línea de color rojo son los riegos potenciales y la línea azul son las salvaguardas existentes.

Figura 37.

Identificación de riesgos por activos



Nota: Elaboración propia. Software PILAR 7.4.2

Se hace una estimación sobre el impacto al que están expuestos los activos del sistema de la empresa.

3.3.7.2 Estimación del Impacto

En esta actividad se determina el impacto potencial y el impacto residual al que está sometido el sistema.

3.3.7.2.1 Impacto potencial

Al que se expone el sistema, tomando en cuenta el valor del activo y la valoración de las amenazas, pero no las salvaguardas que actualmente se despliegan.

Como resultado el sistema PILAR refleja gráficamente los niveles de criticidad que tienen cada uno de los activos

Véase ANEXO 13 Tabla 73 Impacto potencial sobre cada uno de los activos.

Figura 38.

Impacto potencial sobre cada uno de los activos

activo	[D]	[I]	[C]	[A]	[T]
ACTIVOS	[7]	[7]	[7]	[7]	[6]
[IS] Servicios	[7]	[6]	[7]	[7]	[6]
is [SG-SISGECO] SISTEMA DE GESTIÓN SISGECO	[7]	[6]	[7]	[7]	[6]
[E] Equipamiento	[7]	[7]	[7]	[7]	[6]
[SW] Aplicaciones	[7]	[7]	[7]	[7]	[6]
is [SW-SSP] SOFTWARE START SOFT PLANILLAS	[7]	[7]	[7]	[7]	[6]
is [SW-SISCONT] SOFTWARE SISCONT	[7]	[7]	[7]	[7]	[6]
is [SW-GBD] SISTEMA DE GESTION DE BASE DE DATOS	[7]	[7]	[7]	[7]	[6]
is [SW-INTRANET] SISTEMA INTRANET	[4]	[4]	[4]	[4]	[3]
I [SW-ANTIVIRUS] ANTIVIRUS BITDEFENDER	[7]	[7]	[7]		
S [SW-SO] SISTEMA OPERATIVO	[7]	[7]	[7]	[7]	[6]
S [SW-OF] OFIMATICA	[4]	[7]	[7]		
is [BCK] BACKUPS	[7]	[7]	[7]	[7]	[6]
is [SW-CC] CORREO CORPORATIVO	[7]	[7]	[7]	[7]	[6]
[HW] Equipos	[7]	[7]	[7]	[7]	[6]
is [HW-SBD] SERVIDOR BASE DE DATOS	[7]	[7]	[7]	[7]	
id [HW-PC] COMPUTADORA DE ESCRITORIO	[7]	[7]	[7]	[7]	[6]
I [HW-IMP] IMPRESORAS	[4]		[3]	[4]	
is [HW-AP] SERVIDOR APLICACIONES	[7]	[7]	[7]	[7]	
id [HW-SW] SWITCH	[7]	[6]	[6]		
id [HW-CT] CENTRAL IP	[7]	[6]	[6]	[7]	[6]
id [HW-TM] TELEFONIA MOVIL	[5]	[4]	[3]	[5]	
id [HW-FIRE] FIREWALL	[7]	[6]	[6]		
[COM] Comunicaciones	[7]	[7]	[7]	[7]	[6]
P [COM-LAN] RED LAN	[6]	[6]	[6]	[7]	
P [COM-FO] FIBRA OPTICA	[7]	[7]	[7]	[7]	[6]
P [COM-VPN] CONEXION VPN	[7]	[7]	[7]	[7]	[6]
A [COM-WIFI] RED INALAMBRICA	[3]			[6]	
[AUX] Elementos auxiliares	[7]	[7]	[7]		
P [AUX-FA] FUENTES DE ALIMENTACION	[3]				
A [AUX-CCTV] SISTEMA DE CCTV	[7]	[7]	[7]		
P [AUX-AA] AIRE ACONDICIONADO	[4]				
A [AUX-UPS] UPS	[5]				
A [AUX-GE] GRUPO ELECTROGENO	[4]				
P [AUX-CD] CABLEADO DE DATOS	[5]				
[L] Instalaciones	[7]	[7]	[7]		
A [L-ARQ] DATA CENTER OFICINA AREQUIPA	[7]	[7]	[7]		
A [L-SC] DATA CENTER OFICINA SANTA CRUZ	[7]	[7]	[7]		
[P] Personal	[6]	[7]	[7]	[7]	
A [P-AIT] PERSONAL ADMINISTRACION IT	[6]	[7]	[7]	[7]	
A [P-DIT] PERSONAL DESARROLLO IT	[4]	[3]	[5]	[3]	

Nota: Elaboración propia. Software PILAR 7.4.2

3.3.7.2.2 Impacto residual

Es el impacto al que está sometido nuestro sistema, tomando en cuenta el valor de los activos y de las amenazas, así como la efectividad de las salvaguardas implementadas.

Véase ANEXO 14 Tabla 74 Impacto residual

Figura 39.

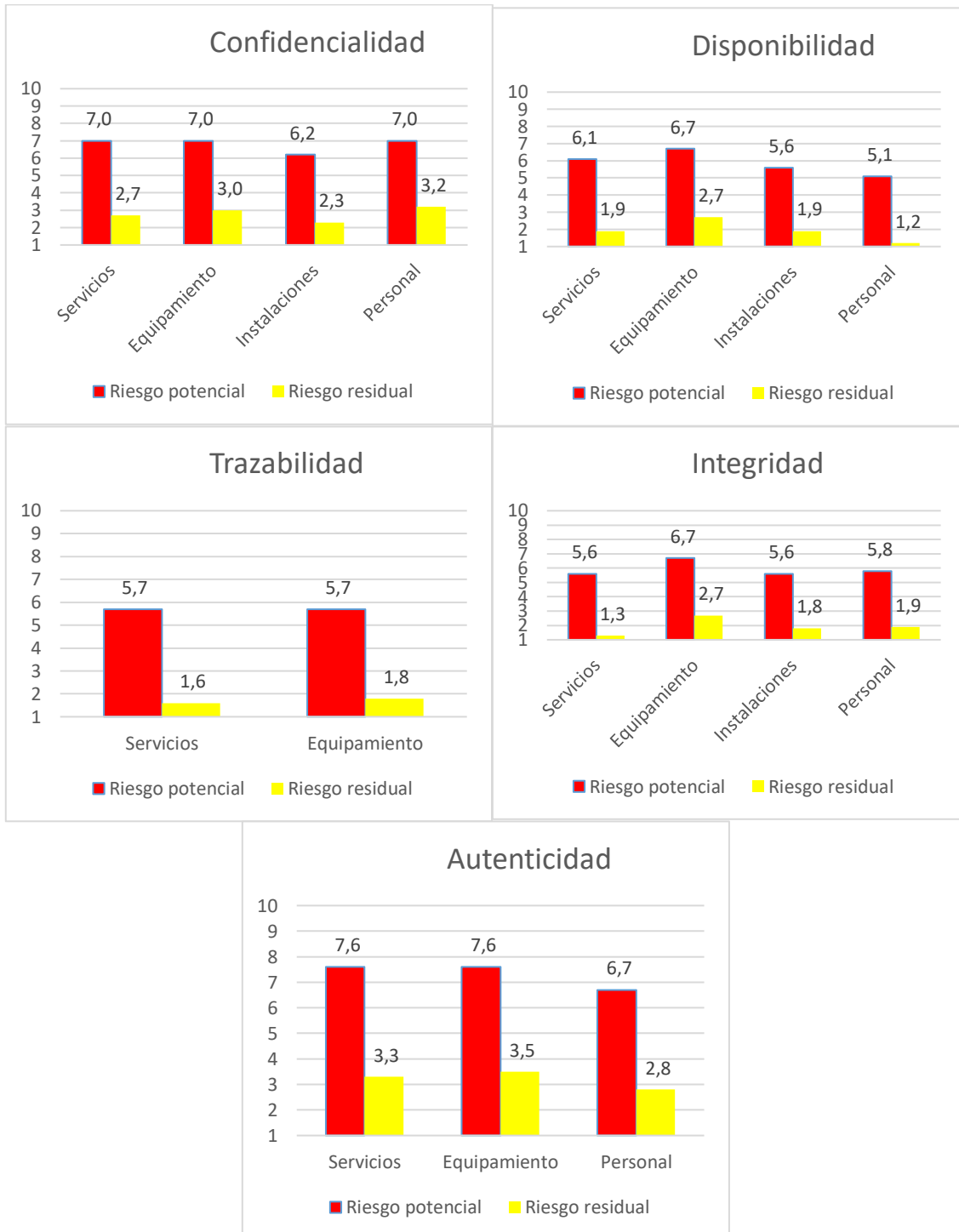
Impacto residual

activo		[D]	[I]	[C]	[A]	[T]
<input type="checkbox"/>	ACTIVOS	[6]	[6]	[6]	[6]	[5]
<input type="checkbox"/>	[IS] Servicios	[6]	[5]	[6]	[6]	[5]
<input type="checkbox"/>	is [SG-SISGECO] SISTEMA DE GESTIÓN SISGECO	[6]	[5]	[6]	[6]	[5]
<input type="checkbox"/>	[E] Equipamiento	[6]	[6]	[6]	[6]	[5]
<input type="checkbox"/>	[SW] Aplicaciones	[6]	[6]	[6]	[6]	[5]
<input type="checkbox"/>	[SW-SSP] SOFTWARE START SOFT PLANILLAS	[6]	[6]	[6]	[6]	[5]
<input type="checkbox"/>	is [SW-SISCONT] SOFTWARE SISCONT	[6]	[6]	[6]	[6]	[5]
<input type="checkbox"/>	is [SW-GBD] SISTEMA DE GESTION DE BASE DE DATOS	[5]	[5]	[5]	[6]	[4]
<input type="checkbox"/>	is [SW-INTRANET] SISTEMA INTRANET	[2]	[2]	[2]	[3]	[1]
<input type="checkbox"/>	I [SW-ANTIVIRUS] ANTIVIRUS BITDEFENDER	[5]	[5]	[5]		
<input type="checkbox"/>	S [SW-SO] SISTEMA OPERATIVO	[5]	[5]	[5]	[6]	[4]
<input type="checkbox"/>	S [SW-OF] OFIMATICA	[2]	[5]	[5]		
<input type="checkbox"/>	is [BCK] BACKUPS	[6]	[6]	[6]	[6]	[5]
<input type="checkbox"/>	is [SW-CC] CORREO CORPORATIVO	[6]	[6]	[6]	[6]	[5]
<input type="checkbox"/>	[HW] Equipos	[6]	[6]	[6]	[6]	[5]
<input type="checkbox"/>	is [HW-SBD] SERVIDOR BASE DE DATOS	[6]	[6]	[6]	[6]	
<input type="checkbox"/>	io [HW-PC] COMPUTADORA DE ESCRITORIO	[6]	[6]	[6]	[6]	[5]
<input type="checkbox"/>	I [HW-IMP] IMPRESORAS	[3]		[2]	[3]	
<input type="checkbox"/>	is [HW-AP] SERVIDOR APLICACIONES	[6]	[6]	[6]	[6]	
<input type="checkbox"/>	io [HW-SW] SWITCH	[6]	[5]	[5]		
<input type="checkbox"/>	io [HW-CT] CENTRAL IP	[6]	[5]	[5]	[6]	[5]
<input type="checkbox"/>	io [HW-TM] TELEFONIA MOVIL	[4]	[3]	[2]	[4]	
<input type="checkbox"/>	io [HW-FIRE] FIREWALL	[6]	[5]	[5]		
<input type="checkbox"/>	[COM] Comunicaciones	[6]	[6]	[6]	[6]	[5]
<input type="checkbox"/>	P [COM-LAN] RED LAN	[5]	[5]	[5]	[6]	
<input type="checkbox"/>	P [COM-FO] FIBRA OPTICA	[6]	[6]	[6]	[6]	[5]
<input type="checkbox"/>	P [COM-VPN] CONEXION VPN	[6]	[6]	[6]	[6]	[5]
<input type="checkbox"/>	A [COM-WIFI] RED INALAMBRICA	[2]			[5]	
<input type="checkbox"/>	[AUX] Elementos auxiliares	[6]	[5]	[5]		
<input type="checkbox"/>	P [AUX-FA] FUENTES DE ALIMENTACION	[2]				
<input type="checkbox"/>	A [AUX-CCTV] SISTEMA DE CCTV	[6]	[5]	[5]		
<input type="checkbox"/>	P [AUX-AA] AIRE ACONDICIONADO	[3]				
<input type="checkbox"/>	A [AUX-UPS] UPS	[4]				
<input type="checkbox"/>	A [AUX-GE] GRUPO ELECTROGENO	[3]				
<input type="checkbox"/>	P [AUX-CD] CABLEADO DE DATOS	[4]				
<input type="checkbox"/>	[L] Instalaciones	[5]	[5]	[5]		
<input type="checkbox"/>	A [L-ARQ] DATA CENTER OFICINA AREQUIPA	[5]	[5]	[5]		
<input type="checkbox"/>	A [L-SC] DATA CENTER OFICINA SANTA CRUZ	[5]	[5]	[5]		
<input type="checkbox"/>	[P] Personal	[5]	[6]	[6]	[6]	
<input type="checkbox"/>	A [P-AIT] PERSONAL ADMINISTRACION IT	[5]	[6]	[6]	[6]	
<input type="checkbox"/>	A [P-DIT] PERSONAL DESARROLLO IT	[3]	[2]	[4]	[2]	

Nota: Elaboración propia. Software PILAR 7.4.2

Figura 40.

Riesgo potencial y riesgo residual sobre los principios de la seguridad



Nota: Elaboración propia.

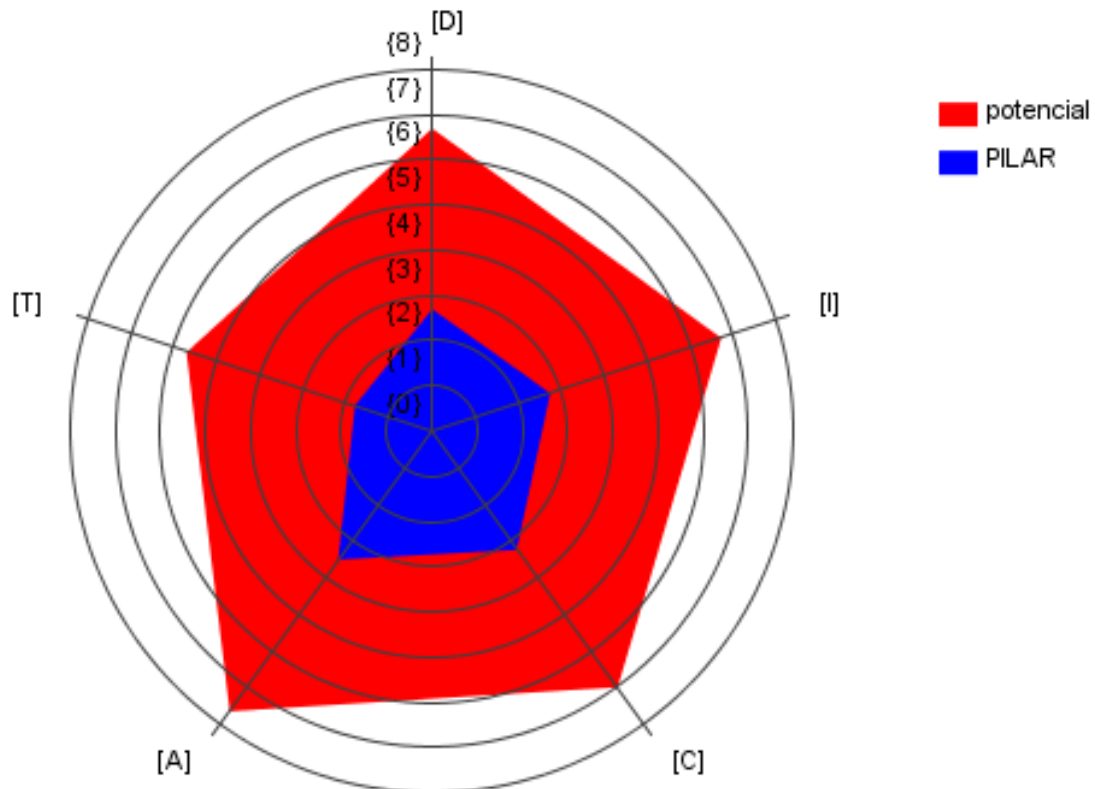
Análisis:

Los resultados mostrados en las figuras 40 y 41 nos muestra el riesgo potencial de las amenazas que tiene la organización, en cada uno de sus principios de la

seguridad, si se implementa la metodología Magerit a través de la EAR PILAR utilizando las salvaguardas propuestas se obtendría una considerable reducción del riesgo potencial del 66%, quedando un riesgo residual de 34%, tal como se muestra en las figuras.

Figura 41.

Riesgo potencial vs riesgo residual en cada uno de los principios de la seguridad



Nota: Elaboración propia. Software PILAR 7.4.2

3.3.8. Proceso de Gestión de los Riesgos

Luego de haber identificado y analizado los pasos anteriores se inicia con el proceso de gestión de los riesgos, determinando impactos y riesgos, además de las consecuencias que estos podrían producir, se debe de determinar hasta que punto la organización está dispuesta a aceptar estos riesgos.

Determinando una calificación a cada riesgo:

Tabla 51.

Calificación de los riesgos

crítico	Se requiere de atención urgente
grave	Se requiere de atención.
apreciable	Puede ser objeto de estudio para su tratamiento.
asumible	No se van a tomar acciones para atajarlo

Nota: Elaboración propia. Tomado de Libro III Guía de técnicas (Administración Electrónica, 2012)

3.3.8.1 Toma de Decisiones

3.3.8.1.1 Identificación de Riesgos Críticos:

En las organizaciones los activos siempre se encuentran comprometidos a riesgos, es por ello la necesidad de saber que activos disponen de un grado superior de riesgo, con el propósito de prevenir que las amenazas se concreten aplicando salvaguardas.

Después de haber estimado los activos y de haber analizado los riesgos al que se encuentran comprometidos, se procede a elegir los activos tienen un grado superior de riesgo, el cual se muestra en la figura 42:

Figura 42.

Identificación de Riesgos Críticos

[DECOINTERIORS] A.6.2. Valores acumulados > A.6.2.2. riesgo

Ver Exportar

potencial current target PILAR

	activo	[D]	[I]	[C]	[A]	[T]
<input type="checkbox"/>	ACTIVOS	(5,6)	(5,8)	(6,2)	(6,7)	(4,6)
<input type="checkbox"/>	[IS] Servicios	(4,8)	(4,6)	(6,0)	(6,6)	(4,4)
<input type="checkbox"/>	[IS] [SG-SISGECO] SISTEMA DE GESTIÓN SISGECO	(4,8)	(4,6)	(6,0)	(6,6)	(4,4)
<input type="checkbox"/>	[E] Equipamiento	(5,6)	(5,8)	(6,2)	(6,7)	(4,6)
<input type="checkbox"/>	[SW] Aplicaciones	(5,5)	(5,8)	(6,2)	(6,7)	(4,6)
<input type="checkbox"/>	[SW-SSP] SOFTWARE START SOFT PLANILLAS	(4,8)	(5,2)	(6,0)	(6,6)	(4,4)
<input type="checkbox"/>	[SW-SISCONT] SOFTWARE SISCONT	(4,8)	(5,2)	(6,0)	(6,6)	(4,4)
<input type="checkbox"/>	[SW-GBD] SISTEMA DE GESTION DE BASE DE DATOS	(4,6)	(5,1)	(5,1)	(4,7)	(4,2)
<input type="checkbox"/>	[SW-INTRANET] SISTEMA INTRANET	(2,9)	(3,3)	(3,3)	(3,0)	(2,4)
<input type="checkbox"/>	[SW-ANTIVIRUS] ANTIVIRUS BITDEFENDER	(4,4)	(4,4)	(5,1)		
<input type="checkbox"/>	[SW-SO] SISTEMA OPERATIVO	(4,6)	(5,1)	(5,1)	(4,7)	(4,2)
<input type="checkbox"/>	[SW-OF] OFIMATICA	(2,6)	(4,4)	(5,1)		
<input type="checkbox"/>	[BCK] BACKUPS	(5,5)	(5,8)	(6,2)	(6,7)	(4,6)
<input type="checkbox"/>	[SW-CC] CORREO CORPORATIVO	(4,6)	(5,6)	(6,0)	(5,6)	(3,8)
<input type="checkbox"/>	[HW] Equipos	(5,6)	(5,3)	(6,2)	(6,7)	(4,6)
<input type="checkbox"/>	[HW-SBD] SERVIDOR BASE DE DATOS	(4,9)	(4,9)	(6,2)	(5,8)	
<input type="checkbox"/>	[HW-PC] COMPUTADORA DE ESCRITORIO	(5,6)	(5,3)	(6,2)	(6,7)	(4,6)
<input type="checkbox"/>	[HW-IMP] IMPRESORAS	(3,7)		(4,4)	(4,9)	
<input type="checkbox"/>	[HW-AP] SERVIDOR APLICACIONES	(4,9)	(4,9)	(6,2)	(5,8)	
<input type="checkbox"/>	[HW-SW] SWITCH	(4,7)	(4,1)	(4,2)		
<input type="checkbox"/>	[HW-CT] CENTRAL IP	(5,4)	(5,2)	(4,5)	(4,8)	(4,4)
<input type="checkbox"/>	[HW-TM] TELEFONIA MOVIL	(4,2)	(4,0)	(2,7)	(3,7)	
<input type="checkbox"/>	[HW-FIRE] FIREWALL	(4,7)	(4,1)	(4,2)		
<input type="checkbox"/>	[COM] Comunicaciones	(5,0)	(4,7)	(5,1)	(4,8)	(3,9)
<input type="checkbox"/>	[COM-LAN] RED LAN	(4,9)	(4,2)	(4,4)	(4,8)	
<input type="checkbox"/>	[COM-FO] FIBRA OPTICA	(5,0)	(4,7)	(5,1)	(4,8)	(3,9)
<input type="checkbox"/>	[COM-VPN] CONEXION VPN	(5,0)	(4,7)	(5,1)	(4,8)	(3,9)
<input type="checkbox"/>	[COM-WIFI] RED INALAMBRICA	(3,2)			(4,2)	
<input type="checkbox"/>	[AUX] Elementos auxiliares	(3,9)	(4,2)	(4,9)		
<input type="checkbox"/>	[AUX-FA] FUENTES DE ALIMENTACION	(2,0)				
<input type="checkbox"/>	[AUX-CCTV] SISTEMA DE CCTV	(3,9)	(4,2)	(4,9)		
<input type="checkbox"/>	[AUX-AA] AIRE ACONDICIONADO	(2,5)				
<input type="checkbox"/>	[AUX-UPS] UPS	(2,8)				
<input type="checkbox"/>	[AUX-GE] GRUPO ELECTROGENO	(2,2)				
<input type="checkbox"/>	[AUX-CD] CABLEADO DE DATOS	(3,2)				
<input type="checkbox"/>	[L] Instalaciones	(4,2)	(4,0)	(4,6)		
<input type="checkbox"/>	[L-ARQ] DATA CENTER OFICINA AREQUIPA	(4,2)	(4,0)	(4,6)		
<input type="checkbox"/>	[L-SC] DATA CENTER OFICINA SANTA CRUZ	(4,2)	(4,0)	(4,6)		
<input type="checkbox"/>	[P] Personal	(3,8)	(4,9)	(6,1)	(5,7)	
<input type="checkbox"/>	[P-AIT] PERSONAL ADMINISTRACION IT	(3,8)	(4,9)	(6,1)	(5,7)	
<input type="checkbox"/>	[P-DIT] PERSONAL DESARROLLO IT	(2,6)	(2,5)	(4,9)	(3,3)	

- 1 + +1 dominio fuente gestionar leyenda

Nota: Elaboración propia. Software PILAR 7.4.2

3.3.8.1.2 Calificación del Riesgo

A continuación se gestionan los activos con riesgos críticos:

Tabla 52.

Sistema de Gestión Sisgeco

Sistema de Gestión Sisgeco
Descripción de criticidad
<p>Este activo es parte de la capa [IS]Servicios, después de haber hallado las amenazas y de seleccionar las salvaguardas anteriormente nombradas se obtienen los resultados siguientes:</p> <ul style="list-style-type: none">✓ Se han encontrado amenazas altas en las dimensiones, teniendo las dimensiones de disponibilidad, integridad y confidencialidad como las que mayor amenaza representan.✓ Los perfiles de accesos es donde mayor riesgo se ha encontrado, ya que no hay un correcto control en el área de TI.✓ Presenta errores muy ocurrentes en cuanto a mantenimiento y puesta en marcha ya que no se realizan en horarios adecuados.✓ Modificaciones accidentales de la información ejecutadas directamente en la base de datos.✓ La suplantación de identidad, es uno de los riesgos más altos que se ha podido determinar.
Controles a emplear
<p>Controles para mitigar los riesgos actuales del activo:</p> <ul style="list-style-type: none">✓ Los cambios y puestas en marcha se realizarán en un horario en el cual no afecte a los usuarios.✓ Toda modificación que se realice en la BD deberá tener la aprobación del Jefe de TI.✓ En cuanto a la suplantación de identidad, cada usuario debe ser el responsable de su ingreso, así mismo se establecerán accesos únicos para cada usuario, determinando su

responsabilidad y perfil de acceso para el cumplimiento de sus funciones.

Nota: Elaboración propia.

Tabla 53.

Software Siscont

Software Siscont
<p>Descripción de criticidad</p> <p>Este activo es parte de la capa [SW]Aplicaciones, despues de haber hallado las amenazas y de seleccionar las salvaguardas anteriormente nombradas se obtienen los resultados siguientes:</p> <ul style="list-style-type: none">✓ Se han encontrado amenazas altas en las dimensiones, teniendo las dimensiones de disponibilidad, integridad y confidencialidad como las que mayor amenaza representan.✓ Los perfiles de accesos es donde mayor riesgo se ha encontrado, ya que no hay un correcto control en el área de TI.✓ Presenta errores muy ocurrentes en cuanto a mantenimiento y puesta en marcha ya que no se realizan en horarios adecuados.✓ Modificaciones accidentales de la información ejecutadas directamente en la base de datos.✓ La suplantación de identidad, es uno de los riesgos mas altos que se ha podido determinar. <p>Controles a emplear</p> <p>Controles para mitigar los riesgos actuales del activo:</p> <ul style="list-style-type: none">✓ Los cambios y puestas en marcha se realizaran en un horario en el cual no afecte a los usuarios.✓ Toda modificación que se realice en la base de datos deberá tener autorización del Jefe de TI y quedará registrado en una bitácota para realizar el seguimiento adecuado.✓ En cuanto a la suplantación de identidad, cada usuario debe ser el responsable de su ingreso.✓ Se deberá establecer accesos únicos para cada usuario, determinando su responsabilidad y perfil de acceso para el cumplimiento de sus funciones.

Nota: Elaboración propia.

Tabla 54.

Software Start Soft Planillas

Software Start Soft Planillas
Descripción de criticidad
<p>Este activo es parte de la capa [SW]Aplicaciones, despues de haber hallado las amenazas y de seleccionar las salvaguardas anteriormente nombradas se obtienen los resultados siguientes:</p> <ul style="list-style-type: none">✓ Se han encontrado amenazas altas en las dimensiones, teniendo las dimensiones de disponibilidad, integridad y confidencialidad como las que mayor amenaza representan.✓ Los perfiles de accesos es donde mayor riesgo se ha encontrado, ya que no hay un correcto control en el área de TI.✓ Presenta errores muy ocurrentes en cuanto a mantenimiento y puesta en marcha ya que no se realizan en horarios adecuados.✓ Modificaciones accidentales de la información ejecutadas directamente en la base de datos.✓ La suplantación de identidad, es uno de los riesgos mas altos que se ha podido determinar.
Controles a emplear
<p>Controles para mitigar los riesgos actuales del activo:</p> <ul style="list-style-type: none">✓ Los cambios y puestas en marcha se realizaran en un horario en el cual no afecte a los usuarios.✓ Toda modificación que se realice en la BD deberá tener autorización del Jefe de TI y quedará registrado en una bitácora para realizar el seguimiento adecuado.✓ En cuanto a la suplantación de identidad, cada usuario debe ser el responsable de su ingreso.

-
- ✓ Se deberá establecer accesos únicos para cada usuario, determinando su responsabilidad y perfil de acceso para el cumplimiento de sus funciones.
-

Nota: Elaboración propia.

Tabla 55.

Sistema de Gestión de Base de Datos

Sistema Gestión de Base de Datos
Descripción de criticidad
<p>Este activo es parte de la capa [SW]Aplicaciones, despues de haber hallado las amenazas y de seleccionar las salvaguardas anteriormente nombradas se obtienen los resultados siguientes:</p> <ul style="list-style-type: none">✓ Se encuentra amenazas altas en las dimensiones, teniendo las dimensiones de disponibilidad, integridad y confidencialidad como las que mayor amenaza representan.✓ Los perfiles de accesos es donde mayor riesgo se ha encontrado, ya que no hay un correcto control en el área de TI.✓ Presenta errores muy ocurrentes en cuanto a mantenimiento y puesta en marcha ya que no se realizan en horarios adecuados.✓ Modificaciones accidentales de la información ejecutadas directamente en la base de datos.✓ La suplantación de identidad, es uno de los riesgos mas altos que se ha podido determinar.
Controles a emplear
<p>Controles para mitigar los riesgos actuales del activo:</p> <ul style="list-style-type: none">✓ Los cambios y puestas en marcha se realizaran en un horario en el cual no afecte a los usuarios.✓ Toda modificación que se realice en la base de datos deberá tener autorización del Jefe de TI y quedará registrado en una bitácora para realizar el seguimiento adecuado.✓ En cuanto a la suplantación de identidad, cada usuario debe ser el responsable de su ingreso.✓ Se deberá establecer accesos únicos para cada usuario, determinando su responsabilidad y perfil de acceso para el cumplimiento de sus funciones.

Nota: Elaboración propia.

Tabla 56.

Sistema Intranet

Sistema Intranet
<p>Descripción de criticidad</p> <p>Este activo es parte de la capa [SW]Aplicaciones, despues de haber hallado las amenazas y de seleccionar las salvaguardas anteriormente nombradas se obtienen los resultados siguientes:</p> <ul style="list-style-type: none">✓ Se encuentra amenazas altas en las dimensiones, teniendo las dimensiones de disponibilidad, integridad y confidencialidad como las que mayor amenaza representan.✓ Los perfiles de accesos es donde mayor riesgo se ha encontrado, ya que no hay un correcto control en el área de TI.✓ Presenta errores muy ocurrentes en cuanto a mantenimiento y puesta en marcha ya que no se realizan en horarios adecuados.✓ Modificaciones accidentales de la información ejecutadas directamente en la base de datos.✓ La suplantación de identidad, es uno de los riesgos mas altos que se ha podido determinar. <p>Controles a emplear</p> <p>Controles para mitigar los riesgos actuales del activo:</p> <ul style="list-style-type: none">✓ Los cambios y puestas en marcha se realizaran en un horario en el cual no afecte a los usuarios.✓ Toda modificación que se realice en la base de datos deberá tener autorización del Jefe de TI y quedará registrado en una bitácora para realizar el seguimiento adecuado.✓ En cuanto a la suplantación de identidad, cada usuario debe ser el responsable de su ingreso.✓ Se deberá establecer accesos únicos para cada usuario, determinando su responsabilidad y perfil de acceso para el cumplimiento de sus funciones.

Nota: Elaboración propia.

Tabla 57.

Servidor de Base de Datos

Servidor de Base de Datos
Descripción de criticidad
<p>Este activo es parte de la capa [SW]Aplicaciones, despues de haber hallado las amenazas y de seleccionar las salvaguardas anteriormente nombradas se obtienen los resultados siguientes:</p> <ul style="list-style-type: none">✓ Se han encontrado amenazas altas en las dimensiones, teniendo las dimensiones de disponibilidad, integridad y confidencialidad como las que mayor amenaza representan.✓ Presenta errores muy ocurrentes en cuanto a mantenimiento y actualización por parte del encargado de la administración de las bases de datos debido a su inexperiencia.✓ Fallos de Hardware
Controles a emplear
<p>Controles para mitigar los riesgos actuales del activo:</p> <ul style="list-style-type: none">✓ Deco Interiors deberá comprometerse a la capacitación del administrador de las BD de esta manera se reduciríamos el riesgo de errores por falta de experiencia.✓ Se deberá realizar mantenimientos preventivos y de manera periódica.

Nota: Elaboración propia.

Tabla 58.

Servidor de Aplicaciones

Servidor de Aplicaciones
Descripción de criticidad
<p>Este activo es parte de la capa [SW]Aplicaciones, despues de haber hallado las amenazas y de seleccionar las salvaguardas anteriormente nombradas se obtienen los resultados siguientes:</p> <ul style="list-style-type: none">✓ Se han encontrado amenazas altas en las dimensiones, teniendo las dimensiones de disponibilidad, integridad y confidencialidad como las que mayor amenaza representan.✓ Acceso Físico de personal no autorizado.✓ Fallos eléctricos.✓ Fallos de Hardware.
Controles a emplear
<p>Controles para mitigar los riesgos actuales del activo:</p> <ul style="list-style-type: none">✓ Deco Interiors deberá comprometerse y garantizar que sólo accederá de manera presencial personal autorizado, así mismo la colocación de cámaras de seguridad.✓ Deco Interiors deberá realizar la compra de UPS para garantizar el correcto apagado del equipo ante problemas eléctricos.✓ Se deberá realizar mantenimientos preventivos y de manera periódica.

Nota: Elaboración propia.

Tabla 59.

Central IP

Central IP
<p>Descripción de criticidad</p> <p>Este activo es parte de la capa [HW]Equipos, despues de haber hallado las amenazas y de seleccionar las salvaguardas anteriormente nombradas se obtienen los resultados siguientes:</p> <ul style="list-style-type: none">✓ Se han encontrado amenazas altas en las dimensiones, teniendo las dimensiones de disponibilidad, integridad y confidencialidad como las que mayor amenaza representan.✓ Se encuentra el mal uso por parte de los usuarios de las líneas de comunicación y de los equipos telefónicos.✓ Interferencia de Red.✓ Fallos de Hardware. <p>Controles a emplear</p> <p>Controles para mitigar los riesgos actuales del activo:</p> <ul style="list-style-type: none">✓ Deco Interiors deberá crear la política de uso correcto de las líneas telefónicas, así mimo deberá brindar la capacitación adecuada a los usuarios para el uso de los equipos.✓ Se deberá realizar el testeo correcto de la red para asegurar que no haya interferencia en la comunicación.✓ Se deberá realizar mantenimientos preventivos y de manera periódica a la Central y a los equipos telefónicos.

Nota: Elaboración propia.

Tabla 60.

Red Lan

Red Lan
<p>Descripción de criticidad</p> <p>Este activo es parte de la capa [COM]Comunicaciones, despues de haber hallado las amenazas y de seleccionar las salvaguardas anteriormente nombradas se obtienen los resultados siguientes:</p> <ul style="list-style-type: none">✓ Se han encontrado amenazas altas en las dimensiones, teniendo las dimensiones de disponibilidad, integridad y confidencialidad como las que mayor amenaza representan.✓ La interrupción del fluido eléctrico se ha dado en varias ocasiones, paralizando las funciones de la organización.✓ El mal uso del servicio de internet ha sido origen de la saturación de la red en reiteradas oportunidades.✓ Fallos de Hardware <p>Controles a emplear</p> <p>Controles para mitigar los riesgos actuales del activo:</p> <ul style="list-style-type: none">✓ Deco Interiors deberá crear la política de uso correcto del servicio de internet.✓ Deco Interiors deberá crear los perfiles de acceso a internet en el firewall, bloqueando las páginas de ocio, streaming y de juegos.✓ Se deberá implementar un grupo electrógeno, el cual permitirá la continuidad del servicio ante una interrupción eléctrica.✓ Se deberá efectuar los mantenimientos correctivos de los equipos de cómputo.

Nota: Elaboración propia.

Tabla 61.

Computadoras de Escritorio

Computadoras de Escritorio
Descripción de criticidad
<p>Este activo es parte de la capa [HW]Equipos, despues de haber hallado las amenazas y de seleccionar las salvaguardas anteriormente nombradas se obtienen los resultados siguientes:</p> <ul style="list-style-type: none">✓ Se han encontrado amenazas altas en las dimensiones, teniendo las dimensiones de disponibilidad, integridad y confidencialidad como las que mayor amenaza representan.✓ La interrupción del fluido eléctrico se ha dado en varias ocasiones, paralizando las funciones de la organización.✓ Acceso de cualquier usuario a los equipos.✓ Los equipos no tienen contraseña✓ Fallos de Hardware
Controles a emplear
<p>Controles para mitigar los riesgos actuales del activo:</p> <ul style="list-style-type: none">✓ Deco Interiors deberá crear la política de uso correcto de los equipos de cómputo.✓ Deco Interiors deberá realizar un correcto uso de AD para que los equipos accedan de acuerdo a los perfiles del usuario que ingresa.✓ Para el acceso al equipo los usuarios deberán loguearse con sus credenciales de acceso.✓ Se deberá realizar el mantenimiento correctivo de los equipos de comunicaciones.

Nota: Elaboración propia.

3.3.9. Plan de Tratamiento de Riesgos

3.3.9.1 Introducción

Se definirán los alcances y objeto de la seguridad de la empresa.

Dividiremos el plan en 2 etapas, en la primera etapa realizaremos una pequeña definición, explicación de los objetivos, sus alcances y resultado producto de la evaluación del riesgo; en la segunda etapa se define el objeto del plan.

3.3.9.2 Primera Etapa

3.3.9.2.1 Definición

En respuesta a los principios que garantizan la seguridad de la información, se realizó el diseño del plan de tratamiento del riesgo.

- ✓ **Confidencialidad de la información;** también conocida como privacidad, hace referencia a que la información sólo debe ser conocida por las personas que necesitan conocerla y que han sido autorizadas para ello. Este principio asegura que la información no va a ser divulgada de manera fortuita o intencionada.
- ✓ **Integridad de la información;** hace referencia a que la información que se encuentra almacenada en los dispositivos o la que se ha transmitido por cualquier canal de comunicación no ha sido manipulada por terceros de manera malintencionada. Esto garantiza que la información no será modificada por personas no autorizadas.
- ✓ **Disponibilidad de la información;** se refiere a que la información debe estar disponible siempre para las personas autorizadas para accederla y tratarla, y además puede recuperarse en caso de que ocurra un incidente de seguridad que cause su pérdida o corrupción.

Es decir; permite que la información esté disponible cuando sea necesario.

3.3.9.2.2 Objetivo del Plan de Tratamiento de los Riesgos

El objetivo es implementar un plan de tratamiento de riesgos que garantice la seguridad y la protección de los activos de la Empresa Deco Interiors SAC administrados por el Área de TI.

3.3.9.2.3 Limitaciones

Este plan será aplicado a los 8 empleados del área de TI, además de todo usuario o empresa externa que realice trabajos directos e indirectos en los activos de la organización.

3.3.9.2.4 Resumen de Resultados del Análisis de Riesgo

Del presente análisis se definió que: sistema de gestión SISGECO (capa de servicios), software Star Soft planillas, software Siscont, sistema de gestión de BD, sistema de Intranet (capa aplicaciones), servidor de aplicaciones y servidor de BD (capa equipos) presentan un alto riesgo; la red LAN, red inalámbrica, fibra óptica (capa de comunicaciones) presentan un riesgo medio, y el data center oficina Arequipa, data center oficina Santa Cruz (capa instalaciones) presentan un bajo riesgo.

3.3.9.3 Segunda Etapa

En el desarrollo del plan de tratamiento de riesgos se han determinado fechas con el objetivo de poder aplicar nuestro plan de tratamiento de riesgos e incrementar la seguridad de la empresa, cada fecha establecida comprenderá de un “**HITO**”, los dos primeros hitos serán ejecutados en diciembre y enero, el 3er y 4to hito será efectuado en el mes de febrero, el 5to será en el mes de

marzo, finalmente el 6to hito será evaluado cada seis meses en cuanto se ejecute el plan.

3.3.9.3.1 HITO 1º : Elaboración de Políticas de Seguridad de la Información

Actividades

- a. Debemos reconocer aquellos riesgos a los que se expone la organización siguiendo la metodología Magerit.
- b. Debemos realizar el análisis de los riesgos de acuerdo a la formalización de las actividades según lo establecido por la metodología Magerit
- c. Se debe documentar las políticas de seguridad, de acuerdo a los objetivos de la organización.
- d. Se capacitará al personal en temas de seguridad de la información.
- e. Se implementan las políticas de seguridad.

Responsables

Los responsables de ejecutar y validar que se cumpla este objetivo en la organización serán, el Jefe de TI y la Gerencia.

Fecha de Realización

Se dará inicio en el mes de diciembre y enero.

3.3.9.3.2 HITO 2º: Mejora de la Seguridad Física

Actividades

- a. Implementación de sistema de acceso biométrico a la oficina y cuarto de servidores del área de TI.
- b. Compra de equipos de video vigilancia, sensor de movimiento, alarma de violación de acceso de puertas y ventanas, sistema contra incendio, entre otros.
- c. Bitácora para el control y registro de los soportes técnicos y mantenimientos preventivos y correctivos de los servidores, PC's y otros activos de computo.
- d. Se realizarán capacitaciones a los usuarios en cuanto a seguridad física.
- e. Restricción y bloqueo de puertos USB y periféricos.

Responsables

Los responsables de ejecutar y validar que se cumpla este objetivo en la organización serán, el Jefe de TI, área de logística y la Gerencia.

Fecha de Realización

Se dará inicio en el mes de diciembre y enero.

3.3.9.3.3 HITO 3º: Mejora de la Seguridad Lógica

Actividades

- a. Se establecerá que la conexión a los sistemas de información será en los itinerarios de oficina.
- b. Realizar bitácora de seguimiento de actividades como; ID de trabajador, horarios de conexión, los registros de acceso a los sistemas informáticos entre otros.
- c. Se realizarán capacitaciones a los usuarios en cuanto a seguridad lógica.
- d. Validación de perfiles de acceso a los sistemas de información de acuerdo a las funciones del trabajador.

Responsables

Los responsables de ejecutar y validar que se cumpla este objetivo en la organización serán, el Jefe de TI, Jefe de Seguridad y la Gerencia. Tener en cuenta nombrar un jefe de seguridad para esta actividad la cual será definido con la Gerencia.

Fecha de Realización

Se dará inicio en el mes de febrero.

3.3.9.3.4 HITO 4º: Mejora de la Seguridad en la Red Lan

Actividades

- a. Se realizará capacitación al personal sobre el manejo del antivirus y las medidas de seguridad que deben de tener en cuenta al utilizar el correo corporativo.
- b. Implementar en el administrador de antivirus escaneos periódicos de cada uno de los equipos informáticos.
- c. Implementar y realizar seguimiento de las actualizaciones del antivirus en cada uno de los equipos informáticos.
- d. Validar en el firewall de acuerdo a los perfiles el correcto acceso a internet.

Responsables

Los responsables de ejecutar y validar que se cumpla este objetivo en la organización serán, el Jefe de TI, Jefe de Seguridad. Tener en cuenta nombrar un jefe de seguridad para esta actividad la cual será definido con la Gerencia.

Fecha de Realización

Se dará inicio en el mes de febrero.

3.3.9.3.5 HITO 5º: Implementación de medidas de Continuidad de los activos de información

Actividades

- a. Se implementarán UPS los cuales permitirán el correcto apagado de los equipos ante fallos eléctricos.
- b. Se contratará almacenamiento virtual, para el correcto resguardo y backup de la información.
- c. Establecer acuerdos contractuales que permita la continuidad de los servicios de la organización.
- d. Realizar tareas diarias de backups de la información y de las BD.
- e. Se deberá establecer el medio y servicio para el respaldo de la información, el cual será definido por el Jefe de TI en conjunto con la Gerencia.

Responsables

Los responsables de ejecutar y validar que se cumpla este objetivo en la organización serán, el Jefe de TI y la Gerencia.

Fecha de Realización

Se dará inicio en el mes de marzo.

3.3.9.3.6 HITO 6º: Revisión del correcto uso de las Políticas de seguridad de Información

Tareas

- a. Se revisarán los sistemas de información para validar que cumplan con los estándares de seguridad.
- b. La Gerencia a través de las jefaturas de cada área deberán validar y asegurar que se cumpla a cabalidad con los métodos de seguridad implementados en cada una de sus dependencias.
- c. En su totalidad las dependencias de la empresa serán tomadas en cuenta para validar si están acatando con las políticas de seguridad implementadas en la empresa.

Responsables

Los responsables de ejecutar y validar que se cumpla este objetivo en la organización serán, el Jefe de TI y el Jefe de Seguridad. Tener en cuenta nombrar un jefe de seguridad para esta actividad la cual será definido con la Gerencia.

Fecha de Realización

Se realizará a partir del sexto mes de implementado el plan.

3.3.9.4 Calendarización

Tabla 62.

Calendarización de Hitos para tratar los principales riesgos

Meses	Diciembre				Enero				Febrero				Marzo				Abril															
tareas/tiempo(semanas)	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4												
3.3.9.3.1 HITO 1º: Elaboración de Políticas de Seguridad de la Información																																
Actividad a	■																															
Actividad b	■																															
Actividad c					■																											
Actividad d									■																							
Actividad e													■																			
3.3.9.3.2 HITO 2º: Mejora de la Seguridad Física																																
Actividad a									■																							
Actividad b													■																			
Actividad c																	■															
Actividad d																																
3.3.9.3.3 HITO 3º: Mejora de la Seguridad Lógica																																
Actividad a																	■															
Actividad b																																
Actividad c																																
3.3.9.3.4 HITO 4º: Mejora de la Seguridad en la Red Lan																																
Actividad a																	■															
Actividad b																																
Actividad c																																
Actividad d																																
3.3.9.3.5 HITO 5º: Implementación de medidas de Continuidad de los activos de información																																
Actividad a																																
Actividad b																																
Actividad c																																
Actividad d																																
Actividad e																																
3.3.9.3.6 HITO 6º: Revisión del correcto uso de las Políticas de seguridad de Información																																
Actividad a																																
Actividad b																																
Actividad c																																

A partir de este HITO se evalúa cada 6 meses

Nota: Elaboración propia.

3.3.9.5 Financiamiento

Tabla 63.

Financiamiento de medidas para tratar los principales riesgos

3.3.9.5 Financiamiento					
Mecanismos de seguridad	Características	Descripción	Cantidad	Costo Unitario	Costo total
Control de acceso biométrico	Utiliza credenciales electrónicas o reconocimiento biométrico para otorgar o denegar el acceso a una instalación. Esto le da al administrador la capacidad inmediata de agregar o eliminar privilegios a cualquier persona y la capacidad de reunir la información sobre el	Acceso al edificio, registro de ingreso. Ingreso a zonas autorizadas	3	S/ 900.00	S/ 2,700.00
Video vigilancia	A través del sistema de video vigilancia se podrá obtener en tiempo real un control de las actividades de los empleados del área de IT.	Acceso de usuarios internos y externos. detección de movimiento. 1 dispositivo por ambiente	7	S/ 142.00	S/ 994.00
Antivirus	Permite la detección y eliminación de malwares, spywares, troyanos entre otros para el correcto uso de los equipos informaticos e informacion a la cual se tiene acceso.	Antivirus, que permita a través de una consola administrativa poder monitorizar a los usuarios, actualizar cada uno de los equipos de computo de la organización.	1	S/ 2,800.00	
Firewall	Ayuda a prevenir y proteger nuestra red privada, de intrusiones o ataques de otras redes, bloqueándole el acceso.	Firewall Fortinet 100D, toda la red	1	S/ 12,000.00	S/ 24,300.00
Backup	Respaldo o copia de la información real para su disposición en caso de alguna incidencia con la información.	Respaldo de 120 Tb de almacenamiento virtual, los costos varían de acuerdo al uso, se colocará un costo aproximado.	1	S/ 9,500.00	
UPS	Permite proveer durante un tiempo energía para evitar daños en los servidores y equipos de cómputo.	UPS para Servidor. UPS para sistema de vigilancia. UPS para sala de comunicaciones.	8	S/ 829.00	S/ 6,632.00
Detección de humo	Permite detectar y prevenir eventos a causa de fuego.	En departamento de TI y data center.	1	S/ 2,700.00	S/ 2,700.00
Extintor	Permite el control ante un amgo de incendio o corto circuito.	En departamento de TI y data center de tipo CO2-PQS(9KG)	7	S/. 139.00	S/ 973.00
TOTAL					S/ 38,299.00

Nota: Elaboración propia.

3.4. Valoración y corroboración de los Resultados

3.4.1. Valoración de los resultados (criterio de expertos)

A través del instrumento elaborado, mostrado en el anexo 3, validado por juicio de expertos en la materia, y cuyo resultado se muestra en el anexo 5, se evaluaron las variables establecidas en el estudio sobre una población de 8 empleados de la organización los cuales se desempeñan en el departamento de informática. Los encuestados son los responsables de asegurar que la información de la empresa se encuentre disponibles, sea confidencial e íntegra, sin embargo, como ya se ha indicado parte de ello se adquiere de las normas y procedimientos instituidos por la organización, y a partir de los resultados obtenidos con la aplicación del instrumento se concluye sobre la influencia que tiene la Metodología Magerit V3 acerca de la seguridad de la información, esto fundamentado en el estudio de las respuestas obtenidas y de la comprobación estadística de la hipótesis planteada, la cual fue indicada en el acápite 3.1.2.

3.4.2. Corroboración estadística de las transformaciones logradas

Determinar la influencia de la Metodología Magerit sobre la Seguridad de la información de la empresa Deco Interiors SAC es el objetivo principal de esta investigación, con el propósito de demostrarle a la referida empresa que en la medida que utilice una metodología para estimar los riesgos y vulnerabilidades al que están inmersos los activos de información, además le permitirá también tomar decisiones con relación al establecimiento de normas y políticas de seguridad. No se puede hablar de transformaciones logradas ya que no se realizó una implementación con lo cual se puede medir los resultados, esto ya dependerá de una decisión de la empresa y de la disponibilidad de recursos tanto económicos como humanos para llevarlo a cabo.

IV. CONCLUSIONES

El análisis de los resultados conseguido permite concluir que:

- Existe una correlación lineal positiva importante de 78% entre la Metodología Magerit V3 y la Seguridad de la información, con un nivel de significancia menor al 0.05 establecida en la investigación, con una influencia del 70.6% de la Metodología Magerit V3 respecto a la Seguridad de la información.
- La empresa Deco Interiors SAC presenta medidas de seguridad en fase de inicio, las cuales han sido implementadas según el criterio de cada empleado de TI, conllevando a que éstas medidas no sean correctamente dirigidas y documentadas, por lo tanto no están siendo aplicadas de manera correcta.
- Se ha constatado la falta de capacitación del personal de la empresa Deco Interiors SAC, en cuanto a seguridad y protección de la información.
- La metodología MAGERIT es de gran apoyo durante los procesos del análisis del riesgo, donde iniciamos con la caracterización de los activos, caracterización de las amenazas, caracterización de las salvaguardas actuales y nos ayuda a implementar futuras salvaguardas para el control y mitigación de riesgos hallados.
- PILAR permitió saber el riesgo e impacto al cual se encuentra sometido los sistemas de información, con los resultados obtenidos podemos determinar el impacto que podría producir la materialización de una amenaza, además sus gráficos permiten relacionar los impactos actuales vs un impacto recomendado por la herramienta.
- Se ha podido dar a conocer que es necesario poner en marcha un plan de gestión y tratamiento de riesgos que consienta atenuar los riesgos y establecer estrategias para disminuir las vulnerabilidades y amenazas a la que están sometidos los activos de información.

V. RECOMENDACIONES

- Se recomienda a la empresa Deco Interiors SAC aplicar la metodología Magerit V3 para gestionar los riesgos y amenazas de los activos de información de la empresa y sobre ello establecer las estrategias que conlleven al aseguramiento de las actividades de la empresa. Esto también se sustenta en la evolución constante tanto de la infraestructura informática como de las formas de vulnerar que las salvaguardas que se diseñan para proteger los activos.
- Se recomienda la capacitación y concientización del personal responsable de la parte informática de la empresa, con lo cual se disminuyen los riesgos entendiendo la relevancia de su contribución en el esfuerzo de conservar un entorno seguro.
- Se recomienda el establecimiento de políticas y normas que aseguren la disponibilidad, confidencialidad, trazabilidad, autenticidad e integridad de la información.

VI. REFERENCIAS

- Amutio, M., Candau, J. & Mañas, J. (2012). Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I – El Método, Ministerio de Hacienda y Administraciones Públicas. Recuperado de: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html
- Amutio, M., Candau, J. & Mañas, J. (2014). MAGERIT- V3, methodology for information systems risk analysis and management. Book I - The Method, Ministerio de Administraciones Públicas. Recuperado de: https://administracionelectronica.gob.es/pae_Home/dam/jcr:80b16a91-75b1-432d-ab23-844a12aab5fc/MAGERIT_v_3_book_1_method_PDF_NIPO_630-14-162-0.pdf
- Arias, F. (2012). *El Proyecto de Investigación. Introducción a la metodología científica*. (6ª Ed). Caracas: Editorial Episteme.
- Ayala, M. (2017). *Sistema de gestión de seguridad de información para mejorar el proceso de gestión del riesgo en un Hospital Nacional, 2017*. (Tesis de grado). Universidad César Vallejo, Lima, Perú. Recuperado de: http://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/13753/Ayala_MMA.pdf?sequence=1&isAllowed=y
- Banda, J. (2019). *Modelo basado en metodologías de gestión de riesgos de TI para contribuir en la mejora de la seguridad de los activos de información en empresas del sector agroindustrial de la región Lambayeque* (Tesis de maestría). Universidad Católica Santo Toribio de Mogrovejo, Chiclayo, Perú. Recuperado de: http://tesis.usat.edu.pe/bitstream/20.500.12423/2159/1/TM_BandaSantistebanJose.pdf
- Behar, D. (2008). *Metodología de la Investigación*. Colombia: Ediciones Shalom. Recuperado de: <http://rdigital.unicv.edu.cv/bitstream/123456789/106/3/Libro%20metodologia%20investigacion%20este.pdf>

- Briceño, C. (2019). *Aplicación de la metodología Magerit para la elaboración de un plan de mejora de la seguridad de los activos de información de la zona especial de desarrollo – ZED Paita* (Tesis de grado). Universidad Nacional de Piura, Piura, Perú. Recuperado de: <http://repositorio.unp.edu.pe/bitstream/handle/UNP/2061/INF-BRI-HUA-2019.pdf?sequence=1&isAllowed=y>
- Calder, A. & Watkins, S. (2008). *A Manager's Guide to Data Security and ISO 27001/ISO 27002*. (4ta ed.). Kogan.
- Cano, J. (2011). El debido cuidado en seguridad de la información. Un ejercicio de virtudes para el responsable de la seguridad de la información. *ISACA Journal*, 2. Recuperado de: SSRN: <https://ssrn.com/abstract=2387914>
- Carrasco, S. (2005). *Metodología de la investigación científica*. Lima: Editorial San Marcos, 2005. 474 pp. ISBN 9972342425.
- Celi, E.K. (2018). *Modelo de gestión de riesgos basados en la norma ISO/IEC 27005 y Metodología Magerit para mejorar la gestión de seguridad de la información en el Hospital Regional de Lambayeque* (Tesis de grado). Universidad Nacional "Pedro Ruíz Gallo", Lambayeque, Perú. Recuperado de: <http://repositorio.unprg.edu.pe/bitstream/handle/UNPRG/3331/BC-TES-TMP-2179.pdf?sequence=1&isAllowed=y>
- Crespo, P. (2016). *Metodología de seguridad de la información para la gestión del riesgo informático aplicable a Mpymes* (Tesis de Maestría). Universidad de Cuenca, Ecuador. Recuperado de: <http://dspace.ucuenca.edu.ec/bitstream/123456789/26105/1/Tesis.pdf>
- Delgado (s/f). *Taller de Implementación de la norma ISO 27001*. Recuperado de: <https://www.pecert.gob.pe/images/publicaciones/4.pdf>
- Duque, A. C. (2017). *Metodología para la gestión de riesgos. Como integrar la seguridad a los objetivos estratégicos de los negocios de una manera costo-beneficiosa*. Recuperado de: http://www.ridssso.com/documentos/muro/207_1469148692_57916e1488c74.pdf

- Espinoza, V. (2019). *Evaluación financiera de la empresa Su Arte, S.A. enfocado en la rentabilidad del negocio en los periodos finalizados 2017-2018* (tesis de pregrado). Universidad Nacional Autónoma de Nicaragua, Managua, Nicaragua. Recuperado de: <https://repositorio.unan.edu.ni/11637/>
- Fernández, A. & García, D. (2016). Complex vs. Simple Asset Modeling Approaches for Information Security Risk Assessment. In The Sixth International Conference on Innovative Computing Technology (INTECH 2016). Recuperado de: <https://scihub.tw/10.1109/INTECH.2016.7845064>
- Gallardo, E. (2017). *Metodología de la investigación*. Huancayo: Universidad Continental.
- Guba, E.G. (1981). Criterios de credibilidad en la investigación naturalista. En Gimeno Sacristán, J. y Pérez Gómez, A. *La Enseñanza: su teoría y su práctica*. Madrid: Akal, 148-165.
- Hernández, R., Fernández, C. & Baptista, P. (2014). *Metodología de la investigación* (6ª Ed.). México D.F: McGraw-Hill / Interamericana Editores, S.A.
- Imbaquingo, D., Herrera-Granda, E., Herrera-Granda, I., Arciniega, S., Guamán, V. & Ortega-Bustamante, M. (2019). Evaluación de sistemas de seguridad informáticos universitarios Caso de Estudio: Sistema de Evaluación Docente. *Revista Ibérica de Sistemas e Tecnologías de Informação*, 349-362. Recuperado de: https://www.researchgate.net/publication/338050855_Evaluacion_de_sistemas_de_seguridad_informaticos_universitarios_Caso_de_Estudio_Sistema_de_Evaluacion_Docente
- ISO (2017). *Glosario de términos*. Recuperado de: <https://www.iso.org/the-iso-survey.html>
- Jara, O. (2018). *Sistema de gestión de seguridad de la información para mejorar el proceso de gestión del riesgo en un gobierno local, 2018*. (Tesis de grado). Universidad César Vallejo, Lima, Perú. Recuperado de: http://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/31209/Jara_MOY.pdf?sequence=1&isAllowed=y

- Molina, M. F. (2015). *Propuesta de un plan de gestión de riesgos de tecnología aplicado en la Escuela Superior Politécnica del Litoral*. (Tesis de maestría). Universidad Politécnica de Madrid, España. Recuperado de: https://www.dit.upm.es/~posgrado/doc/TFM/TFMs2014-2015/TFM_Maria_Fernanda_Molina_Miranda_2015.pdf
- Molina-Miranda, M. (2017). Análisis de riesgos de centro de datos basado en la herramienta Pilar de Magerit. *Espiraes* 1(11). Recuperado de: <http://www.revistaespirales.com/index.php/es/article/view/125/68>
- Motaki, K. (2016). *Risk Analysis and Risk Management in Critical Infrastructures* (Tesis de maestría). University of Piraeus. Recuperado de: http://dione.lib.unipi.gr/xmlui/bitstream/handle/unipi/9741/Motaki_Katerina.pdf?sequence=1&isAllowed=y
- Nieves, A. (2017). *Diseño de un sistema de gestión de la seguridad de la información (sgsi) basados en la norma ISO/IEC 27001:2013* (Tesis de grado). Institución Universitaria Politécnico Grancolombiano, Colombia. Recuperado de: <https://repository.poligran.edu.co/handle/10823/994>
- NIST S 800-30. (2012). Guide for conducting risk assessments. 800–830. Revision 1. Recuperado de: <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf>
- Ñañez, O. (2019). *Modelo de gestión de riesgos de TI basados en la Norma ISO/IEC 27005 y metodología Magerit para mejorar la gestión de seguridad de la información en la Universidad Nacional Toribio Rodríguez de Mendoza – Chachapoyas Perú* (Tesis de maestría). Universidad Nacional Pedro Ruíz Gallo, Lambayeque, Perú. Recuperado de: <http://repositorio.unprg.edu.pe/bitstream/handle/UNPRG/6110/BC-%204020%20%c3%91A%c3%91EZ%20CAMPOS.pdf?sequence=1&isAllowed=y>
- Portal de administración electrónica del Gobierno de España (s/f). *MAGERIT v.3: Metodología de Análisis y Gestión de Riesgos de los*

Sistemas de Información. Recuperado de:
https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

Puyén, V. & Rivas, B. (2018). *Modelo de gestión de riesgos basados en la norma ISO/IEC 27005 y metodología Magerit para mejorar la gestión de seguridad de la información en el Hospital Regional de Lambayeque* (Tesis de grado). Universidad Nacional Pedro Ruíz Gallo, Lambayeque, Perú. Recuperado de:
<http://repositorio.unprg.edu.pe/bitstream/handle/UNPRG/3331/BC-TES-TMP-2179.pdf?sequence=1&isAllowed=y>

Santa Cruz, H. (2016). *Implementación de gestión de riesgos de TI para obtener la certificación ISO 27001 en el Hospital Regional Lambayeque* (Tesis de pregrado). Universidad Señor de Sipán, Chiclayo, Perú. Recuperado de:
http://repositorio.uss.edu.pe/bitstream/handle/uss/160/8%20Milagros_SantaCruz_IF_Gesti%c3%b3n%20de%20Riesgos_Final.pdf?sequence=1&isAllowed=y

Schumacher, M. Fernandez-Buglioni, E., Hybertson, D., Buschmann, F. & Sommerlad, P. (2013). *Security patterns: Integrating security and systems engineering*. England: John Wiley & Sons.

Shameli-Sendi, A., Aghababaei-Barzegar, R., & Cheriet, M. (2016). Taxonomy of Information Security Risk Assessment (ISRA). *Computers & Security*, 57, 14–30.
<http://dx.doi.org/10.1016/j.cose.2015.11.001>

Tarrillo, E. (2016). *Influencia de la Gestión de Riesgo en la seguridad de Activos de Información de la zona Registral III Sede Moyobamba, 2015*. (Tesis de maestría). Universidad César Vallejo, Lima, Perú. Recuperado de:
http://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/1286/tarrillo_se.pdf?sequence=1&isAllowed=y

Taubenberger, S. (2014). *Vulnerability Identification Errors in Security Risk Assessments*. (Tesis doctoral). The Open University, Reino Unido. Recuperado de: <http://oro.open.ac.uk/39626/>

- Viteri, Y., Cano, M., Zambrano, A. & Minaya, C. (2019) desarrollaron el estudio Evaluación de las incidencias y riesgos presentes en la infraestructura tecnológica de la Universidad Laica Eloy Alfaro de Manabí-Ecuador. *Universidad, Ciencia y Tecnología* 21(82), 4-15. Recuperado de: <http://www.uctunexpo.autanabooks.com/index.php/uct/article/view/173/219>
- Administración Electrónica. (10 de 2012). Libro II Catálogo de elementos. Madrid: Ministerio de Hacienda y Administraciones Públicas. Obtenido de <https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html>
- Administración Electrónica. (2012). Libro III - Guía de Técnicas. Madrid: Ministerio de Hacienda y Administraciones Públicas.
- Hernández Sampieri, R. (1997). *METODOLOGÍA DE LA INVESTIGACIÓN*. México: MCGRAW-HILL. Obtenido de https://www.uv.mx/personal/cbustamante/files/2011/06/Metodologia-de-la-Investigaci%C3%83%C2%B3n_Sampieri.pdf
- INCIBE. (16 de 01 de 2017). <https://www.incibe.es>. Obtenido de <https://www.incibe.es/en/node/2789>
- Públicas, M. d. (10 de 2012). <http://administracionelectronica.gob.es/>. Obtenido de <https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html>

VII. ANEXOS

Anexo 1: Matriz de consistencia

Anexo 2: Operacionalización de las variables.

Anexo 3: Instrumentos

Anexo 4: Validación de instrumentos por juicio de expertos

Anexo 4.1 Experto 1

Anexo 4.2 Experto 2

Anexo 4.3 Experto 3

Anexo 5: Validación del aporte práctico de la investigación

Anexo 5.1 Experto 1

Anexo 5.2 Experto 2

Anexo 5.3 Experto 3

Anexo 6: Identificación de activos

Anexo 7: Valoración de activos

Anexo 8: Identificación de amenazas

Anexo 9: Valoración de amenazas

Anexo 10: Identificación y valoración de salvaguardas

Anexo 11: Riesgo potencial de los activos

Anexo 12: Riesgo residual

Anexo 13: Impacto potencial sobre cada uno de los activos

Anexo 14: Impacto residual acumulado

ANEXO N° 1. MATRIZ DE CONSISTENCIA

Manifestaciones del problema	La empresa Deco Interiors SAC solicita involucrar dentro de sus procesos prácticas encaminadas a la protección de la información; las cuales estarán sustentadas en el análisis de riesgos que se deberá realizar a los activos de información de la empresa.
Problema	¿Cómo contribuir a la Seguridad de la Información de la Empresa Deco Interiors SAC?
Causas que originan el Problema	Desconocimiento del impacto que ocasionan los riesgos y amenazas a los que se enfrentan los procesos de la empresa cuando se materializan en situaciones reales.
Objeto de la Investigación	Disminución de los riesgos en la seguridad de la información.
Objetivo General de la Investigación	Determinar la influencia de la Metodología Magerit V3 en la seguridad de información de la empresa Deco Interiors SAC.
Objetivos específicos	<ul style="list-style-type: none"> a) Analizar epistemológicamente la influencia de la Metodología Magerit V3 en el proceso de Seguridad de la Información y su dinámica. b) Diagnosticar la influencia de la Metodología Magerit V3 en el estado actual de la seguridad de la información en la empresa Deco Interiors SAC. c) Determinar la influencia de la Metodología Magerit V3 en la mejora de la seguridad de la empresa Deco Interiors SAC.

	d) Evaluar la influencia de la Metodología Magerit V3 en los cambios provocados en la seguridad de información de la empresa Deco Interiors SAC.
Campo de la investigación	Seguridad de la información.
Título de la Investigación	Influencia de la metodología MAGERIT V3 en la seguridad de información de la empresa Deco Interiors SAC.
Hipótesis	Si se aplica la Metodología Magerit V3, que tenga en cuenta la Cultura y Gestión de riesgo, así como la función del Recurso Humano, entonces se influirá de manera positiva en la seguridad de información de la empresa Deco Interiors SAC.
Variables	Variable independiente: Metodología MAGERIT Variable dependiente: Seguridad de información.

ANEXO N° 2. OPERACIONALIZACIÓN DE LAS VARIABLES

Tabla 64.

Operacionalización de la Variable Independiente Metodología Magerit V3.

Variable	Definición	Dimensión	Indicadores	Ítems	Escala de medición y valores	Rangos % y niveles
Metodología Magerit	Metodología de análisis y gestión de riesgos de tecnologías de la información	Cultura de riesgo de información	• Personal capacitado	1, 2	<ul style="list-style-type: none"> • Nunca • Casi nunca • a veces • siempre • casi siempre 	1 – 49 = Bajo 50 – 77 = Moderado 78 – 100 = Alto
			• Personal concientizado	3, 4, 5		
			• Nivel de planeación	6, 7		
		Gestión de riesgos	• Nivel de identificación	8		
			• Nivel de valoración	9		
		Infraestructura tecnológica	• Disponibilidad tecnológica	10, 11, 12		
			• Conectividad	13		
Recursos humanos	• Nivel de pericia	14				
	• Nivel de conocimiento	15, 16, 17, 18				

Nota. Elaboración propia.

Tabla 65.*Operacionalización de la variable dependiente seguridad de la información de la Empresa Deco Interiors*

Variable	Definición	Dimensión	Indicadores	Ítems	Escala de medición y valores	Rangos % y niveles
Seguridad de la información	Capacidad de las redes o sistemas de información para resistir, con un determinado nivel de confianza, los accidentes, acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad, trazabilidad y confidencialidad de los datos almacenados o transmitidos y de los servicios que dichas redes ofrecen o hacen accesibles.	Seguridad	• Confidencialidad	19	<ul style="list-style-type: none"> • Nunca • Casi nunca • a veces • siempre • casi siempre 	1 – 49 = Bajo 50 – 77 = Moderado 78 – 100 = Alto
			• Integridad	20		
			• Disponibilidad	21, 24, 25		
			• Autenticidad	22		
			• Trazabilidad	23		

Nota. Elaboración propia

ANEXO N° 3 INSTRUMENTO

Cuestionario

Estimado(a) Colaborador:

El presente instrumento tiene como objetivo Determinar la influencia de la Metodología Magerit V3 en la seguridad de información de la empresa Deco Interiors SAC.

Por ello, se le solicita que responda a todos los ítems con veracidad.

Agradeciéndole de antemano su colaboración.

Datos específicos	
1	Nunca
2	Casi nunca
3	A veces
4	Casi siempre
5	Siempre

Variable dependiente: Metodología Magerit V3						
Dimensión 1: Cultura de riesgo de información		1	2	3	4	5
1	¿La empresa le ha proporcionado capacitación sobre el resguardo de información que administra?					
2	¿La empresa le ha proporcionado información sobre los riesgos tecnológicos de la información que administra?					
3	¿Pone en práctica alguna estrategia para la protección de la información?					
4	¿La empresa ha implementado alguna estrategia para concientizar al personal sobre los riesgos e importancia de los activos de información?					
5	¿Se considera comprometido con el resguardo de la información que administra?					
Dimensión 2: Gestión de riesgos		1	2	3	4	5
6	¿La empresa ha implementado alguna estrategia para evaluar los riesgos a los que está sometida la información?					
7	¿La empresa ha determinado los riesgos a los que están sometidos los activos de información?					
8	¿La empresa ha identificado los riesgos sobre la información que afectarían las labores diarias?					
9	¿Se han cuantificado en la empresa los posibles daños en los activos de información?					
Dimensión 3: Infraestructura tecnológica		1	2	3	4	5
10	¿La tecnología de información disponible en la empresa es adecuada para el desarrollo de las actividades?					
11	¿La tecnología de información disponible en la empresa garantiza la seguridad de la información?					
12	¿El servicio de internet disponible en la empresa es adecuado para llevar a cabo sus actividades?					

13	¿Las computadoras están conectadas con la red para enviar y recibir información?					
Dimensión 4: Recursos humanos		1	2	3	4	5
14	¿Su nivel de pericia le permite realizar un adecuado aseguramiento de la información que administra?					
15	¿Requiere de algún tipo de asistencia para resolver problemas informáticos durante sus labores diarias?					
16	¿El servicio de internet le permite ingresar a todas las páginas web que desee?					
17	¿Puede recibir y enviar correos desde su computadora de trabajo?					
18	¿Considera que su nivel de conocimiento en el manejo de la tecnología informática, es sólido?					
Variable Dependiente: Seguridad de la Información						
Dimensión 1: Seguridad		1	2	3	4	5
19	¿La empresa ha establecido políticas o procedimientos para asegurar la confidencialidad de la información?					
20	¿La empresa ha establecido políticas o procedimientos para asegurar la integridad de la información?					
21	¿La empresa ha establecido políticas o procedimientos para asegurar la disponibilidad de la información?					
22	¿La empresa ha establecido políticas o procedimientos para verificar la autenticidad de la información?					
23	¿La empresa ha establecido políticas o procedimientos para verificar la trazabilidad de la información?					
24	¿Existe algún procedimiento para resolver situaciones inesperadas de pérdida de información?					
25	¿Se llevan a cabo respaldos de la información de la empresa como estrategia de resguardo y aseguramiento de la información?					

CUESTIONARIO

8 respuestas

[Publicar análisis](#)

Estimado(a) Colaborador:

NOMBRE:

8 respuestas

MAURICIO PACORA VÁSQUEZ

PAMELA SINCHE ESTEBAN

Clever Paredes Cartagena.

Richard Coria Huamaní

Jorge Marroquín Gamarra

Carlos Daniel Caja Capcha

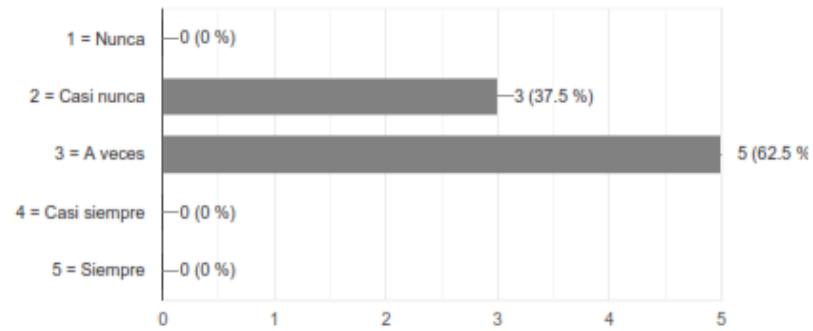
Hairo Marquéz Aguilar

Angélica Cuenca Colchado



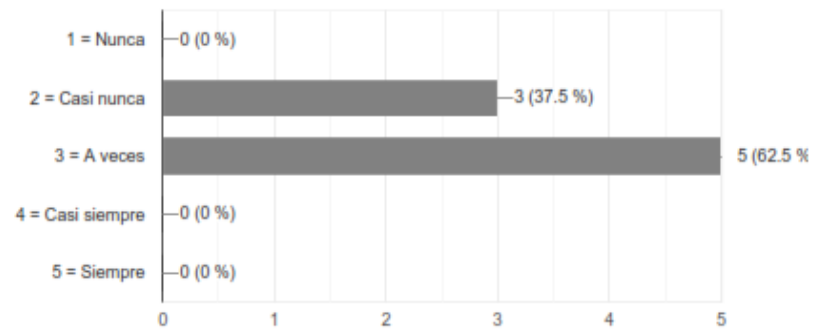
1¿ La empresa le ha proporcionado capacitación sobre el resguardo de información que administra?

8 respuestas



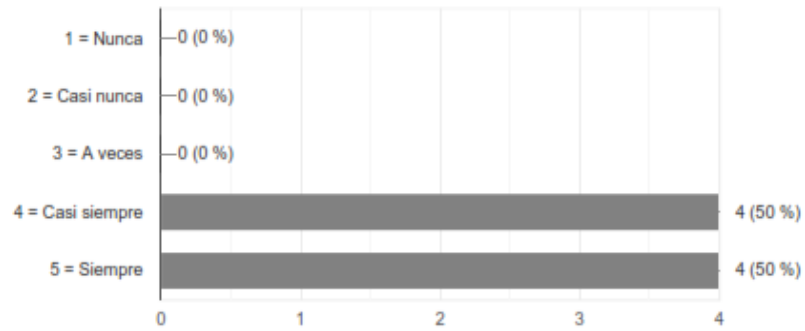
2¿La empresa le ha proporcionado información sobre los riesgos tecnológicos de la información que administra?

8 respuestas



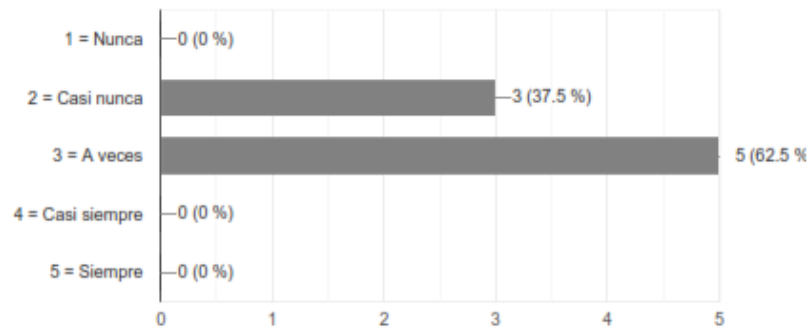
3 ¿Pone en práctica alguna estrategia para la protección de la información?

8 respuestas



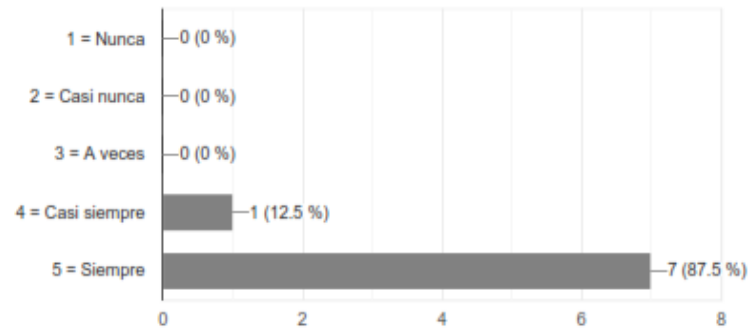
4 ¿La empresa ha implementado alguna estrategia para concientizar al personal sobre los riesgos e importancia de los activos de información?

8 respuestas



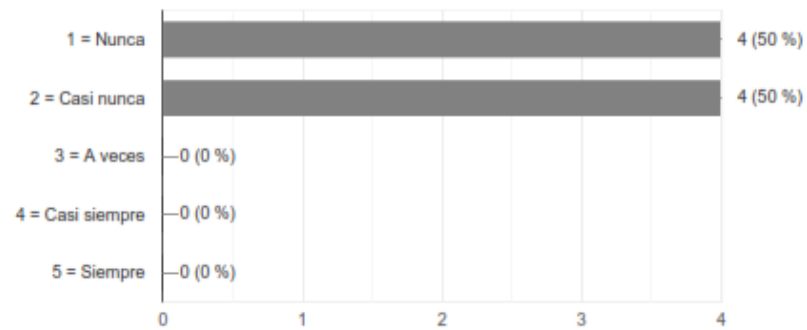
5 ¿Se considera comprometido con el resguardo de la información que administra?

8 respuestas



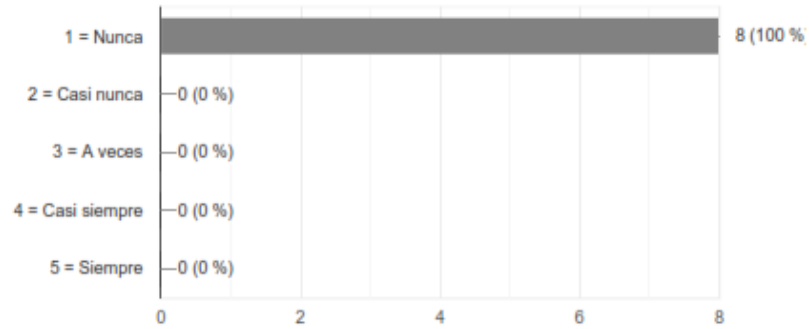
6 ¿La empresa ha implementado alguna estrategia para evaluar los riesgos a los que está sometida la información?

8 respuestas



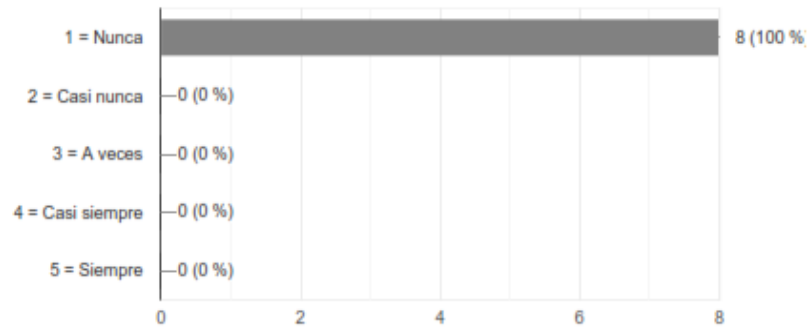
7¿La empresa ha determinado los riesgos a los que están sometidos los activos de información?

8 respuestas



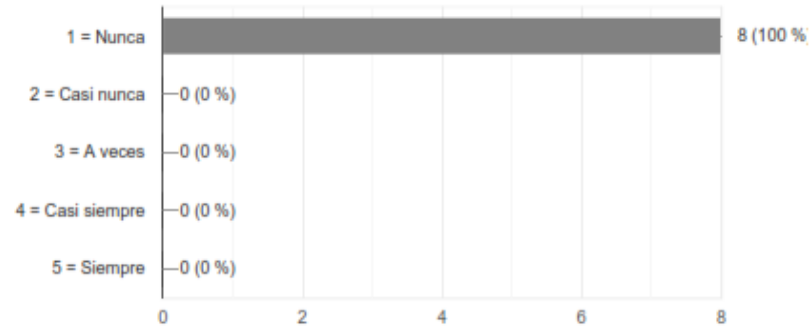
8¿La empresa ha identificado los riesgos sobre la información que afectarían las labores diarias?

8 respuestas



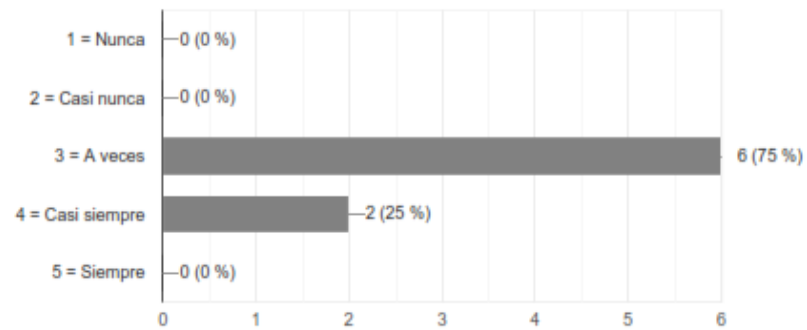
9¿Se han cuantificado en la empresa los posibles daños en los activos de información?

8 respuestas



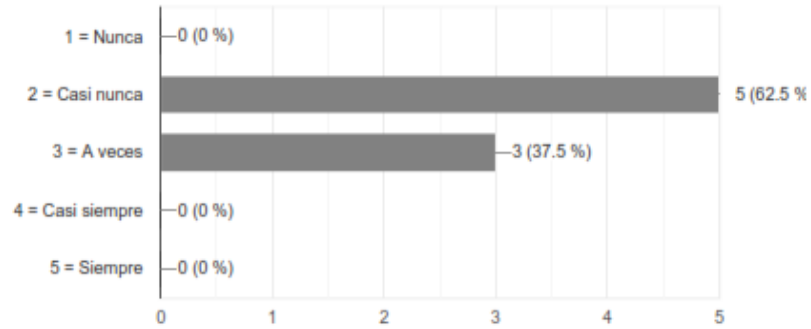
10¿La tecnología de información disponible en la empresa es adecuada para el desarrollo de las actividades?

8 respuestas



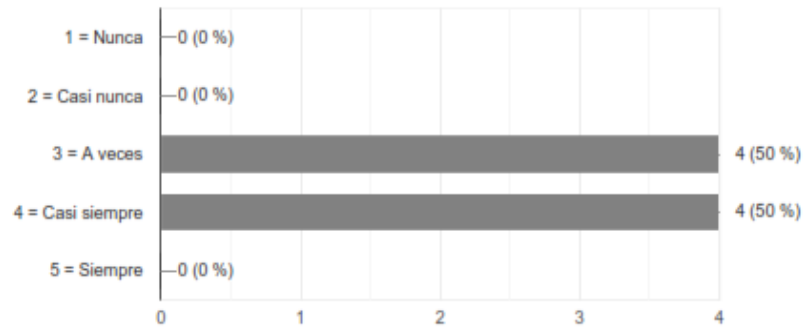
11¿La tecnología de información disponible en la empresa garantiza la seguridad de la información?

8 respuestas



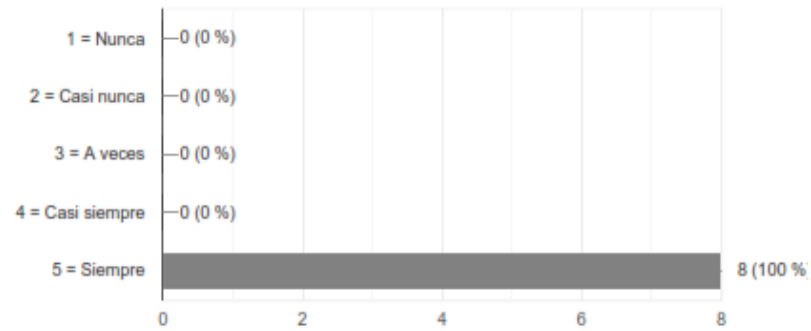
12¿El servicio de internet disponible en la empresa es adecuado para llevar a cabo sus actividades?

8 respuestas



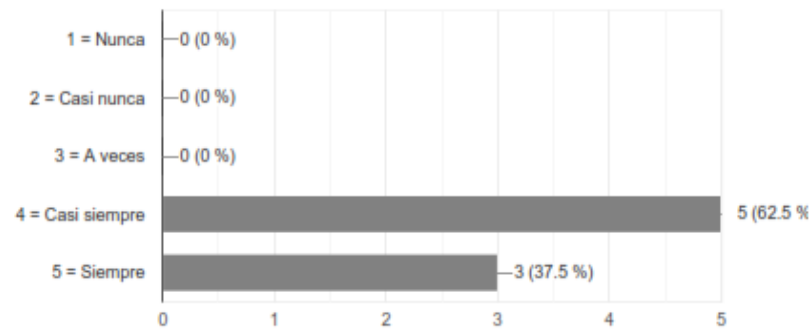
13¿Las computadoras están conectadas con la red para enviar y recibir información?

8 respuestas



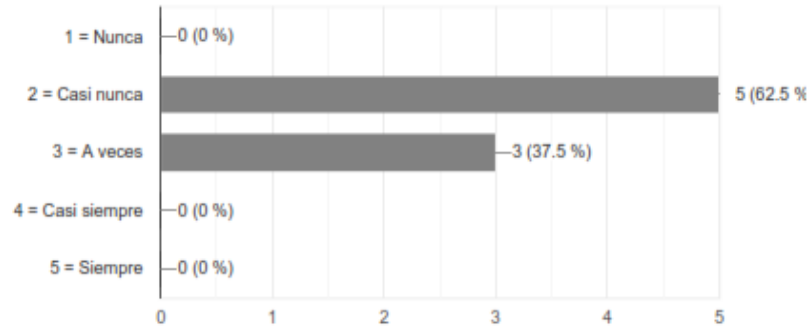
14¿Su nivel de pericia le permite realizar un adecuado aseguramiento de la información que administra?

8 respuestas



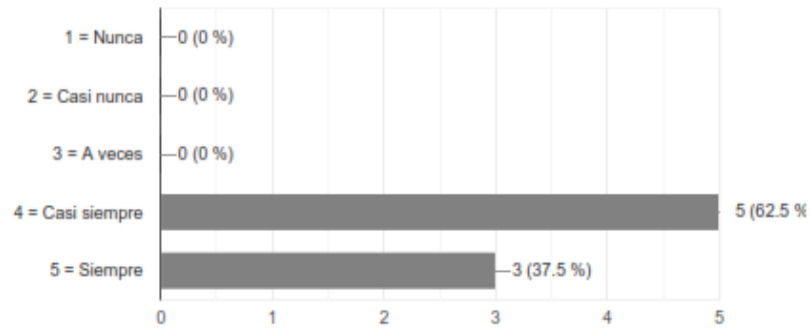
15¿Requiere de algún tipo de asistencia para resolver problemas informáticos durante sus labores diarias?

8 respuestas



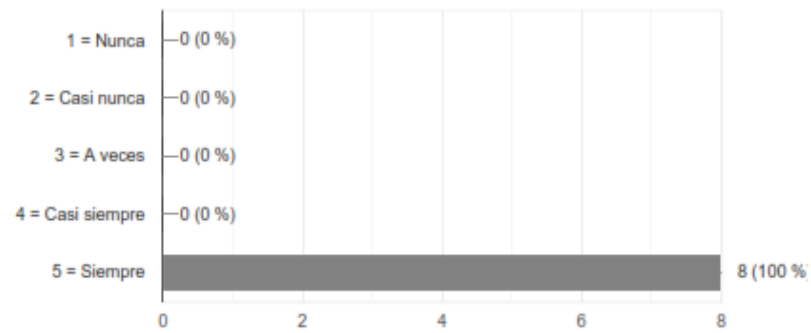
16¿El servicio de internet le permite ingresar a todas las páginas web que desee?

8 respuestas



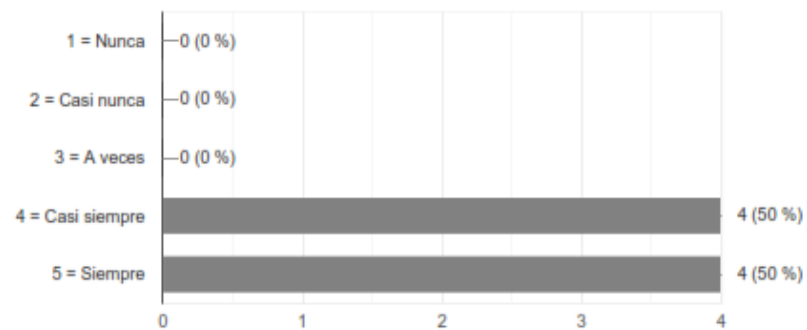
17¿Puede recibir y enviar correos desde su computadora de trabajo?

8 respuestas



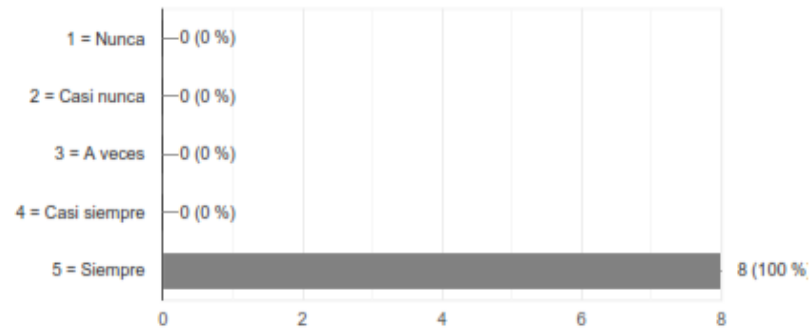
18¿Considera que su nivel de conocimiento en el manejo de la tecnología informática, es sólido?

8 respuestas



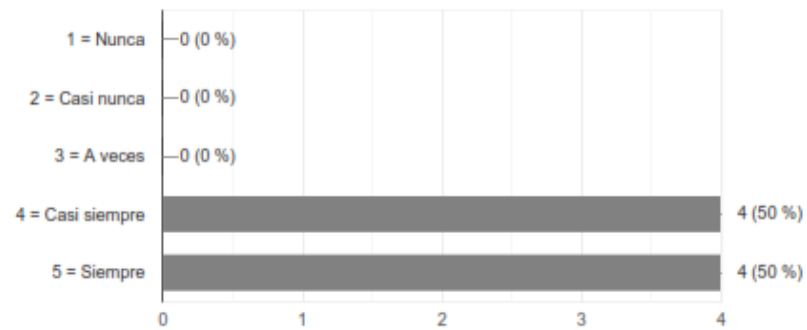
19 ¿La empresa ha establecido políticas o procedimientos para asegurar la confidencialidad de la información?

8 respuestas



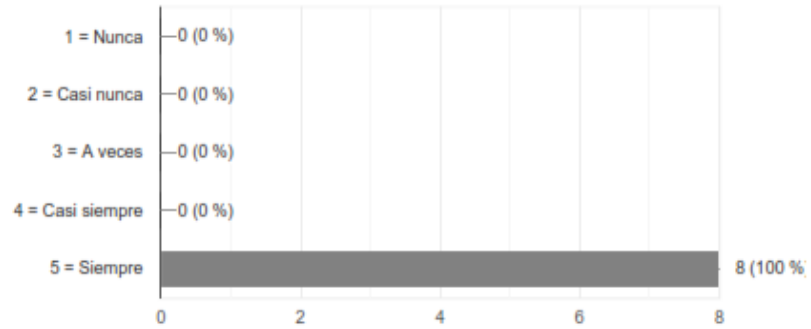
20 ¿La empresa ha establecido políticas o procedimientos para asegurar la integridad de la información?

8 respuestas



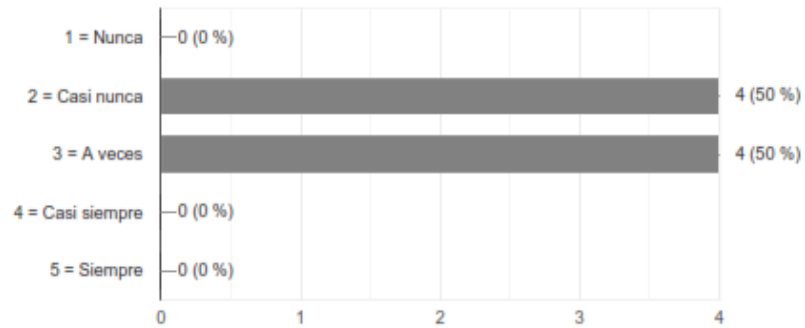
21¿La empresa ha establecido políticas o procedimientos para asegurar la disponibilidad de la información?

8 respuestas



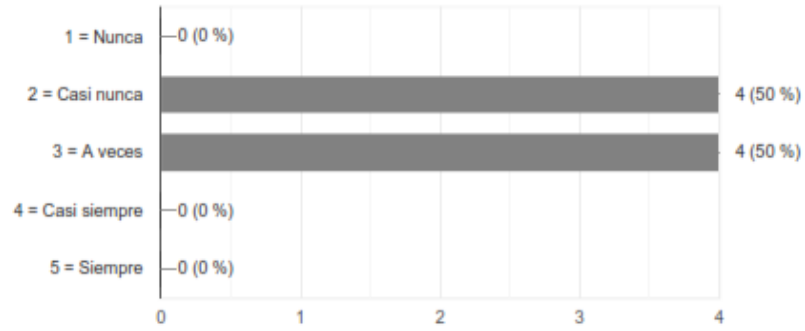
22¿La empresa ha establecido políticas o procedimientos para verificar la autenticidad de la información?

8 respuestas



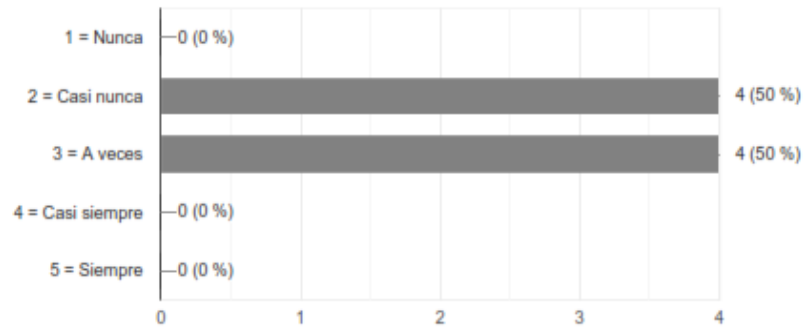
23 ¿La empresa ha establecido políticas o procedimientos para verificar la trazabilidad de la información?

8 respuestas



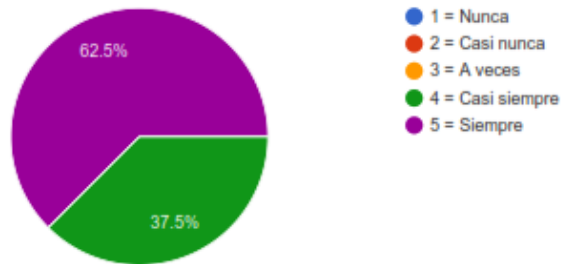
24 ¿Existe algún procedimiento para resolver situaciones inesperadas de pérdida de información?

8 respuestas



25¿Se llevan a cabo respaldos de la información de la empresa como estrategia de resguardo y aseguramiento de la información?

8 respuestas



Google no creó ni aprobó este contenido. [Denunciar abuso](#) - [Condiciones del Servicio](#) - [Política de Privacidad](#)

Google Formularios



ANEXO N° 4 INSTRUMENTO DE VALIDACION NO EXPERIMENTAL POR JUICIO DE EXPERTOS

1. NOMBRE DEL JUEZ		
2.	PROFESIÓN	
	ESPECIALIDAD	
	GRADO ACADÉMICO	
	EXPERIENCIA PROFESIONAL (AÑOS)	
	CARGO	
Título de la Investigación: INFLUENCIA DE LA METODOLOGÍA MAGERIT V3 EN LA SEGURIDAD DE INFORMACIÓN DE LA EMPRESA DECO INTERIORS SAC.		
3. DATOS DEL TESISISTA		
3.1	NOMBRES Y APELLIDOS	Cabrejos Torres, Ramiro
3.2	PROGRAMA DE POSTGRADO	NO
4.	INSTRUMENTO EVALUADO	1. Entrevista () 2. Cuestionario () 3. Lista de Cotejo () 4. Diario de campo ()
5.	OBJETIVOS DEL INSTRUMENTO	<u>GENERAL</u> Determinar la influencia de la Metodología Magerit V3 en la seguridad de información de la empresa Deco Interiors SAC.
		<u>ESPECÍFICOS</u> 1.- Analizar epistemológicamente el proceso de Seguridad de la Información y su dinámica. 2. Diagnosticar el estado actual de la seguridad en la empresa Deco Interiors SAC. 3.- Aplicar la metodología Magerit V3 para mejorar la seguridad de la empresa Deco Interiors SAC. 4.- Evaluar los cambios provocados por la aplicación de la metodología Magerit en la seguridad de información de la empresa Deco Interiors SAC.
A continuación, se le presentan los indicadores en forma de preguntas o propuestas para que Ud. los evalúe marcando con un aspa (x) en "A" si está de ACUERDO o en "D" si está en DESACUERDO, SI ESTÁ EN DESACUERDO POR FAVOR ESPECIFIQUE SUS SUGERENCIAS		
N	DETALLE DE LOS ITEMS DEL INSTRUMENTO	
01	Pregunta del instrumento: ¿La empresa le ha proporcionado capacitación sobre el resguardo de la información que administra? Escala de medición	A() D () SUGERENCIAS:
02	Pregunta del instrumento: ¿La empresa le ha proporcionado información sobre los riesgos tecnológicos de la información que administra? Escala de medición	A() D () SUGERENCIAS:
03	Pregunta del instrumento: ¿Pone en práctica alguna estrategia para la protección de la información? Escala de medición	A() D () SUGERENCIAS:

04	Pregunta del instrumento: ¿La empresa ha implementado alguna estrategia para concientizar al personal sobre los riesgos e importancia de los activos de información? Escala de medición	A() SUGERENCIAS:	D ()
05	Pregunta del instrumento: ¿Se considera comprometido con el resguardo de la información que administra? Escala de medición	A() SUGERENCIAS:	D ()
06	Pregunta del instrumento: ¿La empresa ha implementado alguna estrategia para evaluar los riesgos a los que está sometida la información? Escala de medición	A() SUGERENCIAS:	D ()
07	Pregunta del instrumento: ¿La empresa ha determinado los riesgos a los que están sometidos los activos de información? Escala de medición	A() SUGERENCIAS:	D ()
08	Pregunta del instrumento: ¿La empresa ha identificado los riesgos sobre la información que afectarían las labores diarias? Escala de medición	A() SUGERENCIAS:	D ()
09	Pregunta del instrumento: ¿Se han cuantificado en la empresa los posibles daños en los activos de información? Escala de medición	A() SUGERENCIAS:	D ()
10	Pregunta del instrumento: ¿La tecnología de información disponible en la empresa es adecuada para el desarrollo de las actividades? Escala de medición	A() SUGERENCIAS:	D ()
11	Pregunta del instrumento: ¿La tecnología de información disponible en la empresa garantiza la seguridad de la información? Escala de medición	A() SUGERENCIAS:	D ()
12	Pregunta del instrumento: ¿El servicio de internet disponible en la empresa es adecuado para llevar a cabo sus actividades? Escala de medición	A() SUGERENCIAS:	D ()
13	Pregunta del instrumento: ¿Las computadoras están conectadas con la red para enviar y recibir información? Escala de medición	A() SUGERENCIAS:	D ()
14	Pregunta del instrumento: ¿Su nivel de pericia le permite realizar un adecuado aseguramiento de la información que administra? Escala de medición	A() SUGERENCIAS:	D ()
15	Pregunta del instrumento: ¿Requiere de algún tipo de asistencia para resolver problemas informáticos durante sus labores diarias? Escala de medición	A() SUGERENCIAS:	D ()
16	Pregunta del instrumento: ¿El servicio de internet le permite ingresar a todas las páginas web que desee? Escala de medición	A() SUGERENCIAS:	D ()
17	Pregunta del instrumento: ¿Puede recibir y enviar correos desde su computadora de trabajo? Escala de medición	A() SUGERENCIAS:	D ()

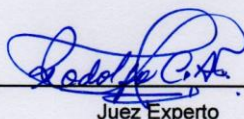
18	Pregunta del instrumento: ¿Considera que su nivel de conocimiento en el manejo de la tecnología informática, es sólido? Escala de medición	A() SUGERENCIAS:	D ()
19	Pregunta del instrumento: ¿La empresa ha establecido políticas o procedimientos para asegurar la confidencialidad de la información? Escala de medición	A() SUGERENCIAS:	D ()
20	Pregunta del instrumento: ¿La empresa ha establecido políticas o procedimientos para asegurar la integridad de la información? Escala de medición	A() SUGERENCIAS:	D ()
21	Pregunta del instrumento: ¿La empresa ha establecido políticas o procedimientos para asegurar la disponibilidad de la información? Escala de medición	A() SUGERENCIAS:	D ()
22	Pregunta del instrumento: ¿La empresa ha establecido políticas o procedimientos para verificar la autenticidad de la información? Escala de medición	A() SUGERENCIAS:	D ()
23	Pregunta del instrumento: ¿La empresa ha establecido políticas o procedimientos para verificar la trazabilidad de la información? Escala de medición	A() SUGERENCIAS:	D ()
24	Pregunta del instrumento: ¿Existe algún procedimiento para resolver situaciones inesperadas de pérdida de información? Escala de medición	A() SUGERENCIAS:	D ()
25	Pregunta del instrumento: ¿Se llevan a cabo respaldos de la información de la empresa como estrategia de resguardo y aseguramiento de la información? Escala de medición	A() SUGERENCIAS:	D ()
PROMEDIO OBTENIDO:		A()	D ():
6 COMENTARIOS GENERALES			
7 OBSERVACIONES			

ANEXO N° 4.1 INSTRUMENTO DE VALIDACION NO EXPERIMENTAL POR JUICIO DE EXPERTOS

1. NOMBRE DEL JUEZ		<i>Rodolfo Manuel Lebas Ayuda</i>
2.	PROFESIÓN	<i>Ingeniero de Computación y Sistemas</i>
	ESPECIALIDAD	<i>Dirección de Tecnologías de la Información</i>
	GRADO ACADÉMICO	<i>Magister</i>
	EXPERIENCIA PROFESIONAL (AÑOS)	<i>25</i>
	CARGO	<i>Sub-Gerente de TI</i>
INSTITUCIÓN DONDE LABORA		<i>Redondo Alimentos S.A.</i>
Título de la Investigación: INFLUENCIA DE LA METODOLOGÍA MAGERIT V3 EN LA SEGURIDAD DE INFORMACIÓN DE LA EMPRESA DECO INTERIORS SAC.		
3. DATOS DEL TESISISTA		
3.1	NOMBRES Y APELLIDOS	Cabrejos Torres, Ramiro
3.2	PROGRAMA DE POSTGRADO	NO
4. INSTRUMENTO EVALUADO	1. Entrevista () 2. Cuestionario (X) 3. Lista de Cotejo () 4. Diario de campo ()	
5. OBJETIVOS DEL INSTRUMENTO	<u>GENERAL</u> Determinar la influencia de la Metodología Magerit V3 en la seguridad de información de la empresa Deco Interiors SAC.	
	<u>ESPECÍFICOS</u> 1.- Analizar epistemológicamente el proceso de Seguridad de la Información y su dinámica 2. Diagnosticar el estado actual de la seguridad en la empresa Deco Interiors SAC 3.- Aplicar la metodología Magerit V3 para mejorar la seguridad de la empresa Deco Interiors SAC 4.- Evaluar los cambios provocados por la aplicación de la metodología Magerit en la seguridad de información de la empresa Deco Interiors SAC.	
A continuación, se le presentan los indicadores en forma de preguntas o propuestas para que Ud. los evalúe marcando con un aspa (x) en "A" si está de ACUERDO o en "D" si está en DESACUERDO, SI ESTÁ EN DESACUERDO POR FAVOR ESPECIFIQUE SUS SUGERENCIAS		
N	6. DETALLE DE LOS ITEMS DEL INSTRUMENTO	
01	Pregunta del instrumento: ¿La empresa le ha proporcionado capacitación sobre el resguardo de la información que administra? Escala de medición	A(X) D () SUGERENCIAS:
02	Pregunta del instrumento: ¿La empresa le ha proporcionado información sobre los riesgos tecnológicos de la información que administra? Escala de medición	A(X) D () SUGERENCIAS:

03	Pregunta del instrumento: ¿Pone en práctica alguna estrategia para la protección de la información? Escala de medición	A(<input checked="" type="checkbox"/>) D () SUGERENCIAS:
04	Pregunta del instrumento: ¿La empresa ha implementado alguna estrategia para concientizar al personal sobre los riesgos e importancia de los activos de información? Escala de medición	A(<input checked="" type="checkbox"/>) D () SUGERENCIAS:
05	Pregunta del instrumento: ¿Se considera comprometido con el resguardo de la información que administra? Escala de medición	A(<input checked="" type="checkbox"/>) D () SUGERENCIAS:
06	Pregunta del instrumento: ¿La empresa ha implementado alguna estrategia para evaluar los riesgos a los que está sometida la información? Escala de medición	A(<input checked="" type="checkbox"/>) D () SUGERENCIAS:
07	Pregunta del instrumento: ¿La empresa ha determinado los riesgos a los que están sometidos los activos de información? Escala de medición	A(<input checked="" type="checkbox"/>) D () SUGERENCIAS:
08	Pregunta del instrumento: ¿La empresa ha identificado los riesgos sobre la información que afectarían las labores diarias? Escala de medición	A(<input checked="" type="checkbox"/>) D () SUGERENCIAS:
09	Pregunta del instrumento: ¿Se han cuantificado en la empresa los posibles daños en los activos de información? Escala de medición	A(<input checked="" type="checkbox"/>) D () SUGERENCIAS:
10	Pregunta del instrumento: ¿La tecnología de información disponible en la empresa es adecuada para el desarrollo de las actividades? Escala de medición	A(<input checked="" type="checkbox"/>) D () SUGERENCIAS:
11	Pregunta del instrumento: ¿La tecnología de información disponible en la empresa garantiza la seguridad de la información? Escala de medición	A(<input checked="" type="checkbox"/>) D () SUGERENCIAS:
12	Pregunta del instrumento: ¿El servicio de internet disponible en la empresa es adecuado para llevar a cabo sus actividades? Escala de medición	A(<input checked="" type="checkbox"/>) D () SUGERENCIAS:
13	Pregunta del instrumento: ¿Las computadoras están conectadas con la red para enviar y recibir información? Escala de medición	A(<input checked="" type="checkbox"/>) D () SUGERENCIAS:
14	Pregunta del instrumento: ¿Su nivel de pericia le permite realizar un adecuado aseguramiento de la información que administra? Escala de medición	A(<input checked="" type="checkbox"/>) D () SUGERENCIAS:
15	Pregunta del instrumento: ¿Requiere de algún tipo de asistencia para resolver problemas informáticos durante sus labores diarias? Escala de medición	A(<input checked="" type="checkbox"/>) D () SUGERENCIAS:
16	Pregunta del instrumento: ¿El servicio de internet le permite ingresar a todas las páginas web que desee? Escala de medición	A(<input checked="" type="checkbox"/>) D () SUGERENCIAS:

17	Pregunta del instrumento: ¿Puede recibir y enviar correos desde su computadora de trabajo? Escala de medición	A(<input checked="" type="checkbox"/>) SUGERENCIAS:	D ()
18	Pregunta del instrumento: ¿Considera que su nivel de conocimiento en el manejo de la tecnología informática, es sólido? Escala de medición	A(<input checked="" type="checkbox"/>) SUGERENCIAS:	D ()
19	Pregunta del instrumento: ¿La empresa ha establecido políticas o procedimientos para asegurar la confidencialidad de la información? Escala de medición	A(<input checked="" type="checkbox"/>) SUGERENCIAS:	D ()
20	Pregunta del instrumento: ¿La empresa ha establecido políticas o procedimientos para asegurar la integridad de la información? Escala de medición	A(<input checked="" type="checkbox"/>) SUGERENCIAS:	D ()
21	Pregunta del instrumento: ¿La empresa ha establecido políticas o procedimientos para asegurar la disponibilidad de la información? Escala de medición	A(<input checked="" type="checkbox"/>) SUGERENCIAS:	D ()
22	Pregunta del instrumento: ¿La empresa ha establecido políticas o procedimientos para verificar la autenticidad de la información? Escala de medición	A(<input checked="" type="checkbox"/>) SUGERENCIAS:	D ()
23	Pregunta del instrumento: ¿La empresa ha establecido políticas o procedimientos para verificar la trazabilidad de la información? Escala de medición	A(<input checked="" type="checkbox"/>) SUGERENCIAS:	D ()
24	Pregunta del instrumento: ¿Existe algún procedimiento para resolver situaciones inesperadas de pérdida de información? Escala de medición	A(<input checked="" type="checkbox"/>) SUGERENCIAS:	D ()
25	Pregunta del instrumento: ¿Se llevan a cabo respaldos de la información de la empresa como estrategia de resguardo y aseguramiento de la información? Escala de medición	A(<input checked="" type="checkbox"/>) SUGERENCIAS:	D ()
PROMEDIO OBTENIDO:		A(<input checked="" type="checkbox"/>)	D ():
6 COMENTARIOS GENERALES			
7 OBSERVACIONES			



Juez Experto

ANEXO N° 4.2 INSTRUMENTO DE VALIDACION NO EXPERIMENTAL POR JUICIO DE EXPERTOS

6. NOMBRE DEL JUEZ		ANA SILVIA CAUNAN SEQUEA
7.	PROFESIÓN	INGENIERIA DE SISTEMAS Y COMPUTACION
	ESPECIALIDAD	INGENIERIA DE SISTEMAS Y COMPUTACION
	GRADO ACADÉMICO	TITULADA
	EXPERIENCIA PROFESIONAL (AÑOS)	7
	CARGO	JEFE DE TI
INSTITUCIÓN DONDE LABORA		PERU Hop SAC
Título de la Investigación: INFLUENCIA DE LA METODOLOGÍA MAGERIT V3 EN LA SEGURIDAD DE INFORMACIÓN DE LA EMPRESA DECO INTERIORS SAC.		
8. DATOS DEL TESISISTA		
3.1	NOMBRES Y APELLIDOS	Cabrejos Torres, Ramiro
3.2	PROGRAMA DE POSTGRADO	NO
9. INSTRUMENTO EVALUADO		5. Entrevista () 6. Cuestionario (X) 7. Lista de Cotejo () 8. Diario de campo ()
10. OBJETIVOS DEL INSTRUMENTO		<u>GENERAL</u> Determinar la influencia de la Metodología Magerit V3 en la seguridad de información de la empresa Deco Interiors SAC. <u>ESPECÍFICOS</u> 1.- Analizar epistemológicamente el proceso de Seguridad de la Información y su dinámica 2. Diagnosticar el estado actual de la seguridad en la empresa Deco Interiors SAC 3.- Aplicar la metodología Magerit V3 para mejorar la seguridad de la empresa Deco Interiors SAC 4.- Evaluar los cambios provocados por la aplicación de la metodología Magerit en la seguridad de información de la empresa Deco Interiors SAC.
A continuación, se le presentan los indicadores en forma de preguntas o propuestas para que Ud. los evalúe marcando con un aspa (x) en "A" si está de ACUERDO o en "D" si está en DESACUERDO, SI ESTÁ EN DESACUERDO POR FAVOR ESPECIFIQUE SUS SUGERENCIAS		
N	7. DETALLE DE LOS ITEMS DEL INSTRUMENTO	
01	Pregunta del instrumento: ¿La empresa le ha proporcionado capacitación sobre el resguardo de la información que administra? Escala de medición	A(X) D() SUGERENCIAS:
02	Pregunta del instrumento: ¿La empresa le ha proporcionado información sobre los riesgos tecnológicos de la información que administra? Escala de medición	A(X) D() SUGERENCIAS:

03	Pregunta del instrumento: ¿Pone en práctica alguna estrategia para la protección de la información? Escala de medición	A(<input checked="" type="checkbox"/>) D() SUGERENCIAS:
04	Pregunta del instrumento: ¿La empresa ha implementado alguna estrategia para concientizar al personal sobre los riesgos e importancia de los activos de información? Escala de medición	A(<input checked="" type="checkbox"/>) D() SUGERENCIAS:
05	Pregunta del instrumento: ¿Se considera comprometido con el resguardo de la información que administra? Escala de medición	A(<input checked="" type="checkbox"/>) D() SUGERENCIAS:
06	Pregunta del instrumento: ¿La empresa ha implementado alguna estrategia para evaluar los riesgos a los que está sometida la información? Escala de medición	A(<input checked="" type="checkbox"/>) D() SUGERENCIAS:
07	Pregunta del instrumento: ¿La empresa ha determinado los riesgos a los que están sometidos los activos de información? Escala de medición	A(<input checked="" type="checkbox"/>) D() SUGERENCIAS:
08	Pregunta del instrumento: ¿La empresa ha identificado los riesgos sobre la información que afectarían las labores diarias? Escala de medición	A(<input checked="" type="checkbox"/>) D() SUGERENCIAS:
09	Pregunta del instrumento: ¿Se han cuantificado en la empresa los posibles daños en los activos de información? Escala de medición	A(<input checked="" type="checkbox"/>) D() SUGERENCIAS:
10	Pregunta del instrumento: ¿La tecnología de información disponible en la empresa es adecuada para el desarrollo de las actividades? Escala de medición	A(<input checked="" type="checkbox"/>) D() SUGERENCIAS:
11	Pregunta del instrumento: ¿La tecnología de información disponible en la empresa garantiza la seguridad de la información? Escala de medición	A(<input checked="" type="checkbox"/>) D() SUGERENCIAS:
12	Pregunta del instrumento: ¿El servicio de internet disponible en la empresa es adecuado para llevar a cabo sus actividades? Escala de medición	A(<input checked="" type="checkbox"/>) D() SUGERENCIAS:
13	Pregunta del instrumento: ¿Las computadoras están conectadas con la red para enviar y recibir información? Escala de medición	A(<input checked="" type="checkbox"/>) D() SUGERENCIAS:
14	Pregunta del instrumento: ¿Su nivel de pericia le permite realizar un adecuado aseguramiento de la información que administra? Escala de medición	A(<input checked="" type="checkbox"/>) D() SUGERENCIAS:
15	Pregunta del instrumento: ¿Requiere de algún tipo de asistencia para resolver problemas informáticos durante sus labores diarias? Escala de medición	A(<input checked="" type="checkbox"/>) D() SUGERENCIAS:
16	Pregunta del instrumento: ¿El servicio de internet le permite ingresar a todas las páginas web que desee? Escala de medición	A(<input checked="" type="checkbox"/>) D() SUGERENCIAS:

17	Pregunta del instrumento: ¿Puede recibir y enviar correos desde su computadora de trabajo? Escala de medición	A(<input checked="" type="checkbox"/>) SUGERENCIAS:	D()
18	Pregunta del instrumento: ¿Considera que su nivel de conocimiento en el manejo de la tecnología informática, es sólido? Escala de medición	A(<input checked="" type="checkbox"/>) SUGERENCIAS:	D()
19	Pregunta del instrumento: ¿La empresa ha establecido políticas o procedimientos para asegurar la confidencialidad de la información? Escala de medición	A(<input checked="" type="checkbox"/>) SUGERENCIAS:	D()
20	Pregunta del instrumento: ¿La empresa ha establecido políticas o procedimientos para asegurar la integridad de la información? Escala de medición	A(<input checked="" type="checkbox"/>) SUGERENCIAS:	D()
21	Pregunta del instrumento: ¿La empresa ha establecido políticas o procedimientos para asegurar la disponibilidad de la información? Escala de medición	A(<input checked="" type="checkbox"/>) SUGERENCIAS:	D()
22	Pregunta del instrumento: ¿La empresa ha establecido políticas o procedimientos para verificar la autenticidad de la información? Escala de medición	A(<input checked="" type="checkbox"/>) SUGERENCIAS:	D()
23	Pregunta del instrumento: ¿La empresa ha establecido políticas o procedimientos para verificar la trazabilidad de la información? Escala de medición	A(<input checked="" type="checkbox"/>) SUGERENCIAS:	D()
24	Pregunta del instrumento: ¿Existe algún procedimiento para resolver situaciones inesperadas de pérdida de información? Escala de medición	A(<input checked="" type="checkbox"/>) SUGERENCIAS:	D()
25	Pregunta del instrumento: ¿Se llevan a cabo respaldos de la información de la empresa como estrategia de resguardo y aseguramiento de la información? Escala de medición	A(<input checked="" type="checkbox"/>) SUGERENCIAS:	D()
PROMEDIO OBTENIDO:		A(<input checked="" type="checkbox"/>)	D():
8	COMENTARIOS GENERALES		
9	OBSERVACIONES		



 Juez Experto

**ANEXO N° 4.3 INSTRUMENTO DE VALIDACION NO EXPERIMENTAL POR
JUICIO DE EXPERTOS**

11. NOMBRE DEL JUEZ		Jose FRANCO FERNANDEZ ZAMORA
12.	PROFESIÓN	INGENIERO DE SISTEMAS
	ESPECIALIDAD	GESTION ESTRATEGICA EMPRESARIAL
	GRADO ACADÉMICO	MAGISTER
	EXPERIENCIA PROFESIONAL (AÑOS)	21
	CARGO	DIRECTOR
INSTITUCIÓN DONDE LABORA		UNIVERSIDAD PRIVADA SAN JUAN BAPTISTA
Título de la Investigación: INFLUENCIA DE LA METODOLOGÍA MAGERIT V3 EN LA SEGURIDAD DE INFORMACIÓN DE LA EMPRESA DECO INTERIORS SAC.		
13. DATOS DEL TESISISTA		
3.1	NOMBRES Y APELLIDOS	Cabrejos Torres, Ramiro
3.2	PROGRAMA DE POSTGRADO	NO
14. INSTRUMENTO EVALUADO		9. Entrevista () 10. Cuestionario (X) 11. Lista de Cotejo () 12. Diario de campo ()
15. OBJETIVOS DEL INSTRUMENTO		<u>GENERAL</u> Determinar la influencia de la Metodología Magerit V3 en la seguridad de información de la empresa Deco Interiors SAC. <u>ESPECÍFICOS</u> 1.- Analizar epistemológicamente el proceso de Seguridad de la Información y su dinámica 2. Diagnosticar el estado actual de la seguridad en la empresa Deco Interiors SAC 3.- Aplicar la metodología Magerit V3 para mejorar la seguridad de la empresa Deco Interiors SAC 4.- Evaluar los cambios provocados por la aplicación de la metodología Magerit en la seguridad de información de la empresa Deco Interiors SAC.
A continuación, se le presentan los indicadores en forma de preguntas o propuestas para que Ud. los evalúe marcando con un aspa (x) en "A" si está de ACUERDO o en "D" si está en DESACUERDO, SI ESTÁ EN DESACUERDO POR FAVOR ESPECIFIQUE SUS SUGERENCIAS		
N	8. DETALLE DE LOS ITEMS DEL INSTRUMENTO	
01	Pregunta del instrumento: ¿La empresa le ha proporcionado capacitación sobre el resguardo de la información que administra? Escala de medición	A(<input checked="" type="checkbox"/>) D() SUGERENCIAS:
02	Pregunta del instrumento: ¿La empresa le ha proporcionado información sobre los riesgos tecnológicos de la información que administra? Escala de medición	A(<input checked="" type="checkbox"/>) D() SUGERENCIAS:

03	Pregunta del instrumento: ¿Pone en práctica alguna estrategia para la protección de la información? Escala de medición	A(<input checked="" type="checkbox"/>) D() SUGERENCIAS:
04	Pregunta del instrumento: ¿La empresa ha implementado alguna estrategia para concientizar al personal sobre los riesgos e importancia de los activos de información? Escala de medición	A(<input checked="" type="checkbox"/>) D() SUGERENCIAS:
05	Pregunta del instrumento: ¿Se considera comprometido con el resguardo de la información que administra? Escala de medición	A(<input checked="" type="checkbox"/>) D() SUGERENCIAS:
06	Pregunta del instrumento: ¿La empresa ha implementado alguna estrategia para evaluar los riesgos a los que está sometida la información? Escala de medición	A(<input checked="" type="checkbox"/>) D() SUGERENCIAS:
07	Pregunta del instrumento: ¿La empresa ha determinado los riesgos a los que están sometidos los activos de información? Escala de medición	A(<input checked="" type="checkbox"/>) D() SUGERENCIAS:
08	Pregunta del instrumento: ¿La empresa ha identificado los riesgos sobre la información que afectarían las labores diarias? Escala de medición	A(<input checked="" type="checkbox"/>) D() SUGERENCIAS:
09	Pregunta del instrumento: ¿Se han cuantificado en la empresa los posibles daños en los activos de información? Escala de medición	A(<input checked="" type="checkbox"/>) D() SUGERENCIAS:
10	Pregunta del instrumento: ¿La tecnología de información disponible en la empresa es adecuada para el desarrollo de las actividades? Escala de medición	A(<input checked="" type="checkbox"/>) D() SUGERENCIAS:
11	Pregunta del instrumento: ¿La tecnología de información disponible en la empresa garantiza la seguridad de la información? Escala de medición	A(<input checked="" type="checkbox"/>) D() SUGERENCIAS:
12	Pregunta del instrumento: ¿El servicio de internet disponible en la empresa es adecuado para llevar a cabo sus actividades? Escala de medición	A(<input checked="" type="checkbox"/>) D() SUGERENCIAS:
13	Pregunta del instrumento: ¿Las computadoras están conectadas con la red para enviar y recibir información? Escala de medición	A(<input checked="" type="checkbox"/>) D() SUGERENCIAS:
14	Pregunta del instrumento: ¿Su nivel de pericia le permite realizar un adecuado aseguramiento de la información que administra? Escala de medición	A(<input checked="" type="checkbox"/>) D() SUGERENCIAS:
15	Pregunta del instrumento: ¿Requiere de algún tipo de asistencia para resolver problemas informáticos durante sus labores diarias? Escala de medición	A(<input checked="" type="checkbox"/>) D() SUGERENCIAS:
16	Pregunta del instrumento: ¿El servicio de internet le permite ingresar a todas las páginas web que desee? Escala de medición	A(<input checked="" type="checkbox"/>) D() SUGERENCIAS:

17	Pregunta del instrumento: ¿Puede recibir y enviar correos desde su computadora de trabajo? Escala de medición	A(<input checked="" type="checkbox"/>) SUGERENCIAS:	D ()
18	Pregunta del instrumento: ¿Considera que su nivel de conocimiento en el manejo de la tecnología informática, es sólido? Escala de medición	A(<input checked="" type="checkbox"/>) SUGERENCIAS:	D ()
19	Pregunta del instrumento: ¿La empresa ha establecido políticas o procedimientos para asegurar la confidencialidad de la información? Escala de medición	A(<input checked="" type="checkbox"/>) SUGERENCIAS:	D ()
20	Pregunta del instrumento: ¿La empresa ha establecido políticas o procedimientos para asegurar la integridad de la información? Escala de medición	A(<input checked="" type="checkbox"/>) SUGERENCIAS:	D ()
21	Pregunta del instrumento: ¿La empresa ha establecido políticas o procedimientos para asegurar la disponibilidad de la información? Escala de medición	A(<input checked="" type="checkbox"/>) SUGERENCIAS:	D ()
22	Pregunta del instrumento: ¿La empresa ha establecido políticas o procedimientos para verificar la autenticidad de la información? Escala de medición	A(<input checked="" type="checkbox"/>) SUGERENCIAS:	D ()
23	Pregunta del instrumento: ¿La empresa ha establecido políticas o procedimientos para verificar la trazabilidad de la información? Escala de medición	A(<input checked="" type="checkbox"/>) SUGERENCIAS:	D ()
24	Pregunta del instrumento: ¿Existe algún procedimiento para resolver situaciones inesperadas de pérdida de información? Escala de medición	A(<input checked="" type="checkbox"/>) SUGERENCIAS:	D ()
25	Pregunta del instrumento: ¿Se llevan a cabo respaldos de la información de la empresa como estrategia de resguardo y aseguramiento de la información? Escala de medición	A(<input checked="" type="checkbox"/>) SUGERENCIAS:	D ()
PROMEDIO OBTENIDO:		A(<input checked="" type="checkbox"/>)	D ():
10 COMENTARIOS GENERALES			
11 OBSERVACIONES			



 Juez Experto

ANEXO N° 5 VALIDACIÓN DEL APOORTE PRÁCTICO DE LA INVESTIGACIÓN ENCUESTA A EXPERTOS

Nombres y Apellidos del validador:

Cargo:

Institución donde trabaja:

Ha sido seleccionado en calidad de experto con el objetivo de valorar la pertinencia en la aplicación del aporte práctico.

DATOS DE LA INVESTIGACIÓN:

TÍTULO DE LA INVESTIGACIÓN	INFLUENCIA DE LA METODOLOGÍA MAGERIT V3 EN LA SEGURIDAD DE INFORMACIÓN DE LA EMPRESA DECO INTERIORS SAC
LINEA DE INVESTIGACIÓN	Infraestructura, Tecnología y Medio Ambiente
NOMBRE DEL TESISISTA	Cabrejos Torres, Ramiro
APOORTE PRÁCTICO	Sobre la base de los resultados del cuestionario y considerando el aporte teórico del marco descrito en capítulos previos, se propone la aplicación de la metodología Magerit en la empresa Deco Interiors SAC para minimizar los riesgos de la implantación y uso de las tecnologías de la información a través de la correspondiente estimación y análisis de los riesgos.

Novedad científica del aporte práctico.

Muy Adecuada (5)	Bastante Adecuada (4)	Adecuada (3)	Poco Adecuada (2)	No Adecuada (1)

Pertinencia de los fundamentos teóricos del aporte práctico.

Muy Adecuada (5)	Bastante Adecuada (4)	Adecuada (3)	Poco Adecuada (2)	No Adecuada (1)

Nivel de argumentación de las relaciones fundamentales aportadas en el desarrollo del aporte práctico.

Muy Adecuada	Bastante Adecuada	Adecuada	Poco Adecuada	No Adecuada

(5)	(4)	(3)	(2)	(1)

Nivel de correspondencia entre las teorías estudiadas y el aporte práctico de la investigación.

Muy Adecuada (5)	Bastante Adecuada (4)	Adecuada (3)	Poco Adecuada (2)	No Adecuada (1)

Claridad en la finalidad de cada una de las acciones del aporte práctico propuesto.

Muy Adecuada (5)	Bastante Adecuada (4)	Adecuada (3)	Poco Adecuada (2)	No Adecuada (1)

Posibilidades de aplicación del aporte práctico.

Muy Adecuada (5)	Bastante Adecuada (4)	Adecuada (3)	Poco Adecuada (2)	No Adecuada (1)

Concepción general del aporte práctico según sus acciones desde la perspectiva de los actores del proceso en el contexto.

Muy Adecuada (5)	Bastante Adecuada (4)	Adecuada (3)	Poco Adecuada (2)	No Adecuada (1)

Significación práctica del aporte.

Muy Adecuada (5)	Bastante Adecuada (4)	Adecuada (3)	Poco Adecuada (2)	No Adecuada (1)

Observaciones generales:

**ANEXO N° 5.1 VALIDACIÓN DEL APOORTE PRÁCTICO DE LA
INVESTIGACIÓN ENCUESTA A EXPERTOS**

Nombres y Apellidos del validador: *Rodolfo Manuel Iribas Agreda*

Cargo: *Sub Gerente de TI.*

Institución donde trabaja: *Redondos Alimentos S.A.*

Ha sido seleccionado en calidad de experto con el objetivo de valorar la pertinencia en la aplicación del aporte práctico.

DATOS DE LA INVESTIGACIÓN:

TITULO DE LA INVESTIGACION	INFLUENCIA DE LA METODOLOGÍA MAGERIT V3 EN LA SEGURIDAD DE INFORMACIÓN DE LA EMPRESA DECO INTERIORS SAC
LINEA DE INVESTIGACION	Infraestructura, Tecnología y Medio Ambiente
NOMBRE DEL TESISISTA	Cabrejos Torres, Ramiro
APOORTE PRÁCTICO	Sobre la base de los resultados del cuestionario y considerando el aporte teórico del marco descrito en capítulos previos, se propone la aplicación de la metodología Magerit en la empresa Deco Interiors SAC para minimizar los riesgos de la implantación y uso de las Tecnologías de la Información a través de la correspondiente estimación y análisis de los riesgos.

Novedad científica del aporte práctico.

Muy Adecuada (5)	Bastante Adecuada (4)	Adecuada (3)	Poco Adecuada (2)	No Adecuada (1)
X				

Pertinencia de los fundamentos teóricos del aporte práctico.

Muy Adecuada (5)	Bastante Adecuada (4)	Adecuada (3)	Poco Adecuada (2)	No Adecuada (1)
X				

Nivel de argumentación de las relaciones fundamentales aportadas en el desarrollo del aporte práctico.

Muy Adecuada (5)	Bastante Adecuada (4)	Adecuada (3)	Poco Adecuada (2)	No Adecuada (1)
X				

Nivel de correspondencia entre las teorías estudiadas y el aporte práctico de la investigación.

Muy Adecuada (5)	Bastante Adecuada (4)	Adecuada (3)	Poco Adecuada (2)	No Adecuada (1)
X				

Claridad en la finalidad de cada una de las acciones del aporte práctico propuesto.

Muy Adecuada (5)	Bastante Adecuada (4)	Adecuada (3)	Poco Adecuada (2)	No Adecuada (1)
	X			

Posibilidades de aplicación del aporte práctico.

Muy Adecuada (5)	Bastante Adecuada (4)	Adecuada (3)	Poco Adecuada (2)	No Adecuada (1)
	X			

Concepción general del aporte práctico según sus acciones desde la perspectiva de los actores del proceso en el contexto.

Muy Adecuada (5)	Bastante Adecuada (4)	Adecuada (3)	Poco Adecuada (2)	No Adecuada (1)
	X			

Significación práctica del aporte.

Muy Adecuada (5)	Bastante Adecuada (4)	Adecuada (3)	Poco Adecuada (2)	No Adecuada (1)
	X			

Observaciones generales: *Analizar la valoración de las vulnerabilidades.*

ANEXO N° 5.2 VALIDACIÓN DEL APORTE PRÁCTICO DE LA INVESTIGACIÓN ENCUESTA A EXPERTOS

Nombres y Apellidos del validador: ANA SILVIA CHUMAN SEGURA
Cargo: JEFE DE TI
Institución donde trabaja: PERU HOP S.A.C
Ha sido seleccionado en calidad de experto con el objetivo de valorar la pertinencia en la aplicación del aporte práctico.

DATOS DE LA INVESTIGACIÓN:

TITULO DE LA INVESTIGACION	INFLUENCIA DE LA METODOLOGÍA MAGERIT V3 EN LA SEGURIDAD DE INFORMACIÓN DE LA EMPRESA DECO INTERIORS SAC
LINEA DE INVESTIGACION	Infraestructura, Tecnología y Medio Ambiente
NOMBRE DEL TESISISTA	Cabrejos Torres, Ramiro
APORTE PRÁCTICO	Sobre la base de los resultados del cuestionario y considerando el aporte teórico del marco descrito en capítulos previos, se propone la aplicación de la metodología Magerit en la empresa Deco Interiors SAC para minimizar los riesgos de la implantación y uso de las Tecnologías de la Información a través de la correspondiente estimación y análisis de los riesgos.

Novedad científica del aporte práctico.

Muy Adecuada (5)	Bastante Adecuada (4)	Adecuada (3)	Poco Adecuada (2)	No Adecuada (1)
X				

Pertinencia de los fundamentos teóricos del aporte práctico.

Muy Adecuada (5)	Bastante Adecuada (4)	Adecuada (3)	Poco Adecuada (2)	No Adecuada (1)
X				

Nivel de argumentación de las relaciones fundamentales aportadas en el desarrollo del aporte práctico.

Muy Adecuada (5)	Bastante Adecuada (4)	Adecuada (3)	Poco Adecuada (2)	No Adecuada (1)
	X			

Nivel de correspondencia entre las teorías estudiadas y el aporte práctico de la investigación.

Muy Adecuada (5)	Bastante Adecuada (4)	Adecuada (3)	Poco Adecuada (2)	No Adecuada (1)
	X			

Claridad en la finalidad de cada una de las acciones del aporte práctico propuesto.

Muy Adecuada (5)	Bastante Adecuada (4)	Adecuada (3)	Poco Adecuada (2)	No Adecuada (1)
X				

Posibilidades de aplicación del aporte práctico.

Muy Adecuada (5)	Bastante Adecuada (4)	Adecuada (3)	Poco Adecuada (2)	No Adecuada (1)
X				

Concepción general del aporte práctico según sus acciones desde la perspectiva de los actores del proceso en el contexto.

Muy Adecuada (5)	Bastante Adecuada (4)	Adecuada (3)	Poco Adecuada (2)	No Adecuada (1)
	X			

Significación práctica del aporte.

Muy Adecuada (5)	Bastante Adecuada (4)	Adecuada (3)	Poco Adecuada (2)	No Adecuada (1)
X				

Observaciones generales:

**ANEXO N° 5.3 VALIDACIÓN DEL APOORTE PRÁCTICO DE LA
INVESTIGACIÓN ENCUESTA A EXPERTOS**

Nombres y Apellidos del validador: JOSÉ FRANCO FERNÁNDEZ ZAMORA

Cargo: DIRECTOR

Institución donde trabaja: UNIVERSIDAD PRIVADA SAN JUAN BAPTISTA

Ha sido seleccionado en calidad de experto con el objetivo de valorar la pertinencia en la aplicación del aporte práctico.

DATOS DE LA INVESTIGACIÓN:

TITULO DE LA INVESTIGACION	INFLUENCIA DE LA METODOLOGÍA MAGERIT V3 EN LA SEGURIDAD DE INFORMACIÓN DE LA EMPRESA DECO INTERIORS SAC
LINEA DE INVESTIGACION	Infraestructura, Tecnología y Medio Ambiente
NOMBRE DEL TESISISTA	Cabrejos Torres, Ramiro
APOORTE PRÁCTICO	Sobre la base de los resultados del cuestionario y considerando el aporte teórico del marco descrito en capítulos previos, se propone la aplicación de la metodología Magerit en la empresa Deco Interiors SAC para minimizar los riesgos de la implantación y uso de las Tecnologías de la Información a través de la correspondiente estimación y análisis de los riesgos.

Novedad científica del aporte práctico.

Muy Adecuada (5)	Bastante Adecuada (4)	Adecuada (3)	Poco Adecuada (2)	No Adecuada (1)
	X			

Pertinencia de los fundamentos teóricos del aporte práctico.

Muy Adecuada (5)	Bastante Adecuada (4)	Adecuada (3)	Poco Adecuada (2)	No Adecuada (1)
X				

Nivel de argumentación de las relaciones fundamentales aportadas en el desarrollo del aporte práctico.

Muy Adecuada (5)	Bastante Adecuada (4)	Adecuada (3)	Poco Adecuada (2)	No Adecuada (1)
X				

Nivel de correspondencia entre las teorías estudiadas y el aporte práctico de la investigación.

Muy Adecuada (5)	Bastante Adecuada (4)	Adecuada (3)	Poco Adecuada (2)	No Adecuada (1)
	X			

Claridad en la finalidad de cada una de las acciones del aporte práctico propuesto.

Muy Adecuada (5)	Bastante Adecuada (4)	Adecuada (3)	Poco Adecuada (2)	No Adecuada (1)
X				

Posibilidades de aplicación del aporte práctico.

Muy Adecuada (5)	Bastante Adecuada (4)	Adecuada (3)	Poco Adecuada (2)	No Adecuada (1)
X				

Concepción general del aporte práctico según sus acciones desde la perspectiva de los actores del proceso en el contexto.

Muy Adecuada (5)	Bastante Adecuada (4)	Adecuada (3)	Poco Adecuada (2)	No Adecuada (1)
	X			

Significación práctica del aporte.

Muy Adecuada (5)	Bastante Adecuada (4)	Adecuada (3)	Poco Adecuada (2)	No Adecuada (1)
X				

Observaciones generales:

ANEXO N° 6 IDENTIFICACIÓN DE ACTIVOS

Tabla 66.

Identificación de activos

CAPAS	ACTIVOS
[S] SERVICIOS	[SG-SISGECO] SISTEMA DE GESTIÓN SISGECO
	[SW-SSP] SOFTWARE STAR SOFT PLANILLAS
	[SW-SISCONT] SOFTWARE SISCONT
	[SW-GBD] SISTEMA DE GESTION DE BASE DE DATOS
[SW] APLICACIONES	[SW-INTRANET] SISTEMA INTRANET
	[SW-ANTIVIRUS] ANTIVIRUS BITDEFENDER
	[SW-SO] SISTEMA OPERATIVO
	[SW-OF] OFIMATICA
	[BCK] BACKUPS
	[SW-CC] CORREO CORPORATIVO
	[HW-SBD] SERVIDOR DE BASE DE DATOS
	[HW-PC] COMPUTADORA DE ESCRITORIO
	[HW-IMP] IMPRESORAS
[HW] EQUIPOS	[HW-AP] SERVIDOR APLICACIONES
	[HW-SW] SWITCH
	[HW-CT] CENTRAL IP
	[HW-TM] TELEFONIA MOVIL
	[HW-FIRE] FIREWALL
	[COM-LAN] RED LAN
[COM] COMUNICACIONES	[COM-FO] FIBRA OPTICA
	[COM-VPN] CONEXIÓN VPN
	[COM-WIFI] RED INALAMBRICA
	[AUX-FA] FUENTES DE ALIMENTACION
	[AUX-CCTV] SISTEMA DE CCTV
[AUX] ELEMENTOS AUXILIARES	[AUX-AA] AIRE ACONDICIONADO
	[AUX-UPS] UPS
	[AUX-GE] GRUPO ELECTROGENO
	[AUX-CD] CABLEADO DE DATOS
[L] INSTALACIONES	[L-ARQ] DATA CENTER OFICINA AREQUIPA
	[L-SC] DATA CENTER OFICINA SANTA CRUZ
[P] PERSONAL	[P-AIT] PERSONAL ADMINISTRACION IT
	[P-DIT] PERSONAL DESARROLLO IT

Nota: Elaboración propia.

ANEXO N° 7 VALORACIÓN DE ACTIVOS

Tabla 67.

Valoración de activos

CAPAS	ACTIVOS	[D]	[I]	[C]	[A]	[T]
[S] SERVICIOS	[SG-SISGECO] SISTEMA DE GESTIÓN SISGECO	[10]	[9]	[10]	[10]	[9]
	[SW-SSP] SOFTWARE STAR SOFT PLANILLAS	[8]	[8]	[9]	[9]	[8]
	[SW-SISCONT] SOFTWARE SISCONT	[9]	[8]	[8]	[8]	[7]
	[SW-GBD] SISTEMA DE GESTION DE BASE DE DATOS	[10]	[9]	[9]	[8]	[7]
[SW] APLICACIONES	[SW-INTRANET] SISTEMA INTRANET	[7]	[7]	[7]	[6]	[6]
	[SW-ANTIVIRUS] ANTIVIRUS BITDEFENDER	[8]	[5]	[5]	[5]	[5]
	[SW-SO] SISTEMA OPERATIVO	[6]		[1]	[5]	[1]
	[SW-OF] OFIMATICA	[5]	[3]			
	[BCK] BACKUPS	[10]	[9]	[8]	[9]	[7]
	[SW-CC] CORREO CORPORATIVO	[9]	[8]	[8]	[9]	[7]
	[HW-SBD] SERVIDOR DE BASE DE DATOS	[10]	[9]	[9]	[8]	[8]
	[HW-PC] COMPUTADORA DE ESCRITORIO	[9]	[7]	[7]	[8]	
	[HW-IMP] IMPRESORAS	[7]		[7]	[7]	
[HW] EQUIPOS	[HW-AP] SERVIDOR APLICACIONES	[10]	[9]	[9]	[9]	[8]
	[HW-SW] SWITCH	[9]				
	[HW-CT] CENTRAL IP	[9]	[8]	[7]	[8]	
	[HW-TM] TELEFONIA MOVIL	[8]	[8]	[7]	[8]	
	[HW-FIRE] FIREWALL	[10]				
[COM] COMUNICACIONES	[COM-LAN] RED LAN	[9]	[9]	[9]	[9]	
	[COM-FO] FIBRA OPTICA	[10]	[9]	[9]		
	[COM-VPN] CONEXIÓN VPN	[9]	[9]	[9]	[9]	
	[COM-WIFI] RED INALAMBRICA	[7]			[9]	
[AUX] ELEMENTOS AUXILIARES	[AUX-FA] FUENTES DE ALIMENTACION	[6]				
	[AUX-CCTV] SISTEMA DE CCTV	[7]		[8]	[8]	
	[AUX-AA] AIRE ACONDICIONADO	[8]				
	[AUX-UPS] UPS	[9]				
	[AUX-GE] GRUPO ELECTROGENO	[8]				
	[AUX-CD] CABLEADO DE DATOS	[8]				
[L] INSTALACIONES	[L-ARQ] DATA CENTER OFICINA AREQUIPA	[9]	[8]	[8]	[8]	
	[L-SC] DATA CENTER OFICINA SANTA CRUZ	[9]	[8]	[8]	[8]	
[P] PERSONAL	[P-AIT] PERSONAL ADMINISTRACION IT	[9]	[8]	[8]	[8]	
	[P-DIT] PERSONAL DESARROLLO IT	[8]	[6]	[8]	[6]	

Nota: Elaboración propia.

ANEXO N° 8 IDENTIFICACIÓN DE AMENAZAS

Tabla 68.

Identificación de amenazas

CAPA	ACTIVOS	AMENAZAS
		Total
		[I.5] Avería de origen físico o lógico
		[E.1] Errores de los usuarios
		[E.2] Errores del administrador del sistema / de la seguridad
		[E.8] Difusión de software dañino
		[E.15] Alteración de la información
		[E.18] Destrucción de la información
		[E.19] Fugas de información
		[E.20] Vulnerabilidades de los programas (software)
		[E.24] Caída del sistema por agotamiento de los recursos
		[E.28] Indisponibilidad del personal
[S] SERVICIOS	[SG-SISGECO] SISTEMA DE GESTIÓN SISGECO	[A.5] Suplantación de la identidad
		[A.6] Abuso de privilegios de acceso
		[A.7] Uso no previsto
		[A.8] Difusión de software dañino
		[A.11] Acceso no autorizado
		[A.13] Repudio (negación de actuaciones)
		[A.15] Modificación de la información
		[A.18] Destrucción de la información
		[A.19] Revelación de información
		[A.22] Manipulación de programas
		[A.24] Denegación de servicio
		[A.28] Indisponibilidad del personal
		[A.29] Extorsión
		[A.30] Ingeniería social (picaresca)
		Total
		[I.5] Avería de origen físico o lógico
		[E.1] Errores de los usuarios
		[E.2] Errores del administrador del sistema / de la seguridad
		[E.8] Difusión de software dañino
		[E.15] Alteración de la información
		[E.18] Destrucción de la información
		[E.19] Fugas de información
		[E.20] Vulnerabilidades de los programas (software)
		[E.24] Caída del sistema por agotamiento de los recursos
		[E.28] Indisponibilidad del personal
[SW] APLICACIONES	[SW-SSP] SOFTWARE STAR SOFT PLANILLAS	[A.5] Suplantación de la identidad
		[A.6] Abuso de privilegios de acceso
		[A.7] Uso no previsto
		[A.8] Difusión de software dañino

	<p>[A.11] Acceso no autorizado</p> <p>[A.13] Repudio (negación de actuaciones)</p> <p>[A.15] Modificación de la información</p> <p>[A.18] Destrucción de la información</p> <p>[A.19] Revelación de información</p> <p>[A.22] Manipulación de programas</p> <p>[A.24] Denegación de servicio</p> <p>[A.28] Indisponibilidad del personal</p> <p>[A.29] Extorsión</p> <p>[A.30] Ingeniería social (picaresca)</p> <p>Total</p> <p>[I.5] Avería de origen físico o lógico</p> <p>[E.1] Errores de los usuarios</p> <p>[E.2] Errores del administrador del sistema / de la seguridad</p> <p>[E.8] Difusión de software dañino</p> <p>[E.15] Alteración de la información</p> <p>[E.18] Destrucción de la información</p> <p>[E.19] Fugas de información</p> <p>[E.20] Vulnerabilidades de los programas (software)</p> <p>[E.24] Caída del sistema por agotamiento de los recursos</p> <p>[E.28] Indisponibilidad del personal</p>
[SW-SISCONT] SOFTWARE SISCONT	<p>[A.5] Suplantación de la identidad</p> <p>[A.6] Abuso de privilegios de acceso</p> <p>[A.7] Uso no previsto</p> <p>[A.8] Difusión de software dañino</p> <p>[A.11] Acceso no autorizado</p> <p>[A.13] Repudio (negación de actuaciones)</p> <p>[A.15] Modificación de la información</p> <p>[A.18] Destrucción de la información</p> <p>[A.19] Revelación de información</p> <p>[A.22] Manipulación de programas</p> <p>[A.24] Denegación de servicio</p> <p>[A.28] Indisponibilidad del personal</p> <p>[A.29] Extorsión</p> <p>[A.30] Ingeniería social (picaresca)</p> <p>Total</p> <p>[I.5] Avería de origen físico o lógico</p> <p>[E.1] Errores de los usuarios</p> <p>[E.2] Errores del administrador del sistema / de la seguridad</p> <p>[E.8] Difusión de software dañino</p> <p>[E.15] Alteración de la información</p> <p>[E.18] Destrucción de la información</p> <p>[E.19] Fugas de información</p> <p>[E.20] Vulnerabilidades de los programas (software)</p> <p>[E.24] Caída del sistema por agotamiento de los recursos</p> <p>[E.28] Indisponibilidad del personal</p>
[SW-GBD] SISTEMA DE GESTION DE BASE DE DATOS	<p>[E.28] Indisponibilidad del personal</p>

	<ul style="list-style-type: none"> [A.5] Suplantación de la identidad [A.6] Abuso de privilegios de acceso [A.7] Uso no previsto [A.8] Difusión de software dañino [A.11] Acceso no autorizado [A.13] Repudio (negación de actuaciones) [A.15] Modificación de la información [A.18] Destrucción de la información [A.19] Revelación de información [A.22] Manipulación de programas [A.24] Denegación de servicio [A.28] Indisponibilidad del personal [A.29] Extorsión [A.30] Ingeniería social (picaresca) Total [I.5] Avería de origen físico o lógico [E.1] Errores de los usuarios [E.2] Errores del administrador del sistema / de la seguridad [E.8] Difusión de software dañino [E.15] Alteración de la información [E.18] Destrucción de la información [E.19] Fugas de información [E.20] Vulnerabilidades de los programas (software) [E.24] Caída del sistema por agotamiento de los recursos
<p>[SW-INTRANET] SISTEMA INTRANET</p>	<ul style="list-style-type: none"> [E.28] Indisponibilidad del personal [A.5] Suplantación de la identidad [A.6] Abuso de privilegios de acceso [A.7] Uso no previsto [A.8] Difusión de software dañino [A.11] Acceso no autorizado [A.13] Repudio (negación de actuaciones) [A.15] Modificación de la información [A.18] Destrucción de la información [A.19] Revelación de información [A.22] Manipulación de programas [A.24] Denegación de servicio [A.28] Indisponibilidad del personal [A.29] Extorsión [A.30] Ingeniería social (picaresca) Total [I.5] Avería de origen físico o lógico [E.8] Difusión de software dañino [E.15] Alteración de la información [E.19] Fugas de información [E.20] Vulnerabilidades de los programas (software) [E.28] Indisponibilidad del personal
<p>[SW-ANTIVIRUS] ANTIVIRUS BITDEFENDER</p>	<ul style="list-style-type: none"> [A.8] Difusión de software dañino

	<ul style="list-style-type: none"> [A.15] Modificación de la información [A.18] Destrucción de la información [A.19] Revelación de información [A.22] Manipulación de programas [A.28] Indisponibilidad del personal [A.29] Extorsión [A.30] Ingeniería social (picaresca) Total [I.5] Avería de origen físico o lógico [E.1] Errores de los usuarios [E.2] Errores del administrador del sistema / de la seguridad [E.8] Difusión de software dañino [E.15] Alteración de la información [E.18] Destrucción de la información [E.19] Fugas de información [E.20] Vulnerabilidades de los programas (software) [E.24] Caída del sistema por agotamiento de los recursos [E.28] Indisponibilidad del personal
[SW-SO] SISTEMA OPERATIVO	<ul style="list-style-type: none"> [A.5] Suplantación de la identidad [A.6] Abuso de privilegios de acceso [A.7] Uso no previsto [A.8] Difusión de software dañino [A.11] Acceso no autorizado [A.13] Repudio (negación de actuaciones) [A.15] Modificación de la información [A.18] Destrucción de la información [A.19] Revelación de información [A.22] Manipulación de programas [A.24] Denegación de servicio [A.28] Indisponibilidad del personal [A.29] Extorsión [A.30] Ingeniería social (picaresca) Total [E.8] Difusión de software dañino [E.15] Alteración de la información [E.19] Fugas de información [E.20] Vulnerabilidades de los programas (software)
[SW-OF] OFIMÁTICA	<ul style="list-style-type: none"> [A.8] Difusión de software dañino [A.15] Modificación de la información [A.19] Revelación de información [A.22] Manipulación de programas [A.29] Extorsión [A.30] Ingeniería social (picaresca) Total
[BCK] BACKUPS	<ul style="list-style-type: none"> [N.1] Fuego [N.2] Daños por agua [N.*] Desastres naturales

**[SW-CC] CORREO
CORPORATIVO**

[I.1] Fuego
[I.2] Daños por agua
[I.*] Desastres industriales
[I.3] Contaminación medioambiental
[I.4] Contaminación electromagnética
[I.5] Avería de origen físico o lógico
[I.6] Corte del suministro eléctrico
[I.7] Condiciones inadecuadas de temperatura o humedad
[I.10] Degradación de los soportes de almacenamiento de la información
[E.1] Errores de los usuarios
[E.2] Errores del administrador del sistema / de la seguridad
[E.18] Destrucción de la información
[E.19] Fugas de información
[E.23] Errores de mantenimiento / actualización de equipos (hardware)
[E.24] Caída del sistema por agotamiento de los recursos
[E.25] Pérdida de equipos
[A.5] Suplantación de la identidad
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.11] Acceso no autorizado
[A.13] Repudio (negación de actuaciones)
[A.15] Modificación de la información
[A.18] Destrucción de la información
[A.23] Manipulación del hardware
[A.24] Denegación de servicio
[A.25] Robo de equipos
[A.26] Ataque destructivo
Total
[I.5] Avería de origen físico o lógico
[I.9] Interrupción de otros servicios o suministros esenciales
[E.8] Difusión de software dañino
[E.15] Alteración de la información
[E.18] Destrucción de la información
[E.19] Fugas de información
[E.20] Vulnerabilidades de los programas (software)
[E.28] Indisponibilidad del personal
[A.5] Suplantación de la identidad
[A.6] Abuso de privilegios de acceso
[A.8] Difusión de software dañino
[A.11] Acceso no autorizado
[A.13] Repudio (negación de actuaciones)
[A.15] Modificación de la información
[A.18] Destrucción de la información
[A.19] Revelación de información
[A.22] Manipulación de programas

		[A.24] Denegación de servicio
		[A.28] Indisponibilidad del personal
		[A.29] Extorsión
		[A.30] Ingeniería social (picaresca)
		Total
		[N.1] Fuego
		[N.2] Daños por agua
		[N.*] Desastres naturales
		[I.1] Fuego
		[I.2] Daños por agua
		[I.*] Desastres industriales
		[I.3] Contaminación medioambiental
		[I.4] Contaminación electromagnética
		[I.5] Avería de origen físico o lógico
		[I.6] Corte del suministro eléctrico
		[I.7] Condiciones inadecuadas de temperatura o humedad
		[E.8] Difusión de software dañino
		[E.15] Alteración de la información
		[E.19] Fugas de información
		[E.20] Vulnerabilidades de los programas (software)
		[E.23] Errores de mantenimiento / actualización de equipos (hardware)
	[HW-SBD] SERVIDOR DE BASE DE DATOS	[E.24] Caída del sistema por agotamiento de los recursos
		[E.25] Pérdida de equipos
		[E.28] Indisponibilidad del personal
[HW] EQUIPOS		[A.5] Suplantación de la identidad
		[A.6] Abuso de privilegios de acceso
		[A.7] Uso no previsto
		[A.8] Difusión de software dañino
		[A.11] Acceso no autorizado
		[A.15] Modificación de la información
		[A.18] Destrucción de la información
		[A.19] Revelación de información
		[A.22] Manipulación de programas
		[A.23] Manipulación del hardware
		[A.24] Denegación de servicio
		[A.25] Robo de equipos
		[A.26] Ataque destructivo
		[A.28] Indisponibilidad del personal
		[A.29] Extorsión
		[A.30] Ingeniería social (picaresca)
		Total
		[N.1] Fuego
		[N.2] Daños por agua
		[N.*] Desastres naturales
	[HW-PC] COMPUTADORA DE ESCRITORIO	[I.1] Fuego
		[I.2] Daños por agua
		[I.*] Desastres industriales

**[HW-IMP]
IMPRESORAS**

- [I.3] Contaminación medioambiental
 - [I.4] Contaminación electromagnética
 - [I.5] Avería de origen físico o lógico
 - [I.6] Corte del suministro eléctrico
 - [I.7] Condiciones inadecuadas de temperatura o humedad
 - [E.1] Errores de los usuarios
 - [E.2] Errores del administrador del sistema / de la seguridad
 - [E.8] Difusión de software dañino
 - [E.15] Alteración de la información
 - [E.18] Destrucción de la información
 - [E.19] Fugas de información
 - [E.20] Vulnerabilidades de los programas (software)
 - [E.23] Errores de mantenimiento / actualización de equipos (hardware)
 - [E.24] Caída del sistema por agotamiento de los recursos
 - [E.25] Pérdida de equipos
 - [E.28] Indisponibilidad del personal
 - [A.5] Suplantación de la identidad
 - [A.6] Abuso de privilegios de acceso
 - [A.7] Uso no previsto
 - [A.8] Difusión de software dañino
 - [A.11] Acceso no autorizado
 - [A.13] Repudio (negación de actuaciones)
 - [A.15] Modificación de la información
 - [A.18] Destrucción de la información
 - [A.19] Revelación de información
 - [A.22] Manipulación de programas
 - [A.23] Manipulación del hardware
 - [A.24] Denegación de servicio
 - [A.25] Robo de equipos
 - [A.26] Ataque destructivo
 - [A.28] Indisponibilidad del personal
 - [A.29] Extorsión
 - [A.30] Ingeniería social (picaresca)
 - Total
 - [N.1] Fuego
 - [N.2] Daños por agua
 - [N.*] Desastres naturales
 - [I.1] Fuego
 - [I.2] Daños por agua
 - [I.*] Desastres industriales
 - [I.3] Contaminación medioambiental
 - [I.4] Contaminación electromagnética
 - [I.5] Avería de origen físico o lógico
 - [I.6] Corte del suministro eléctrico
 - [I.7] Condiciones inadecuadas de temperatura o humedad
-

**[HW-AP]
SERVIDOR
APLICACIONES**

- [E.1] Errores de los usuarios
 - [E.2] Errores del administrador del sistema / de la seguridad
 - [E.18] Destrucción de la información
 - [E.19] Fugas de información
 - [E.23] Errores de mantenimiento / actualización de equipos (hardware)
 - [E.24] Caída del sistema por agotamiento de los recursos
 - [E.25] Pérdida de equipos
 - [E.28] Indisponibilidad del personal
 - [A.5] Suplantación de la identidad
 - [A.6] Abuso de privilegios de acceso
 - [A.7] Uso no previsto
 - [A.11] Acceso no autorizado
 - [A.18] Destrucción de la información
 - [A.19] Revelación de información
 - [A.23] Manipulación del hardware
 - [A.24] Denegación de servicio
 - [A.25] Robo de equipos
 - [A.26] Ataque destructivo
 - [A.28] Indisponibilidad del personal
 - [A.29] Extorsión
 - [A.30] Ingeniería social (picaresca)
 - Total
 - [N.1] Fuego
 - [N.2] Daños por agua
 - [N.*] Desastres naturales
 - [I.1] Fuego
 - [I.2] Daños por agua
 - [I.*] Desastres industriales
 - [I.3] Contaminación medioambiental
 - [I.4] Contaminación electromagnética
 - [I.5] Avería de origen físico o lógico
 - [I.6] Corte del suministro eléctrico
 - [I.7] Condiciones inadecuadas de temperatura o humedad
 - [E.8] Difusión de software dañino
 - [E.15] Alteración de la información
 - [E.19] Fugas de información
 - [E.20] Vulnerabilidades de los programas (software)
 - [E.23] Errores de mantenimiento / actualización de equipos (hardware)
 - [E.24] Caída del sistema por agotamiento de los recursos
 - [E.25] Pérdida de equipos
 - [E.28] Indisponibilidad del personal
 - [A.5] Suplantación de la identidad
 - [A.6] Abuso de privilegios de acceso
 - [A.7] Uso no previsto
 - [A.8] Difusión de software dañino
-

	<p>[A.11] Acceso no autorizado</p> <p>[A.15] Modificación de la información</p> <p>[A.18] Destrucción de la información</p> <p>[A.19] Revelación de información</p> <p>[A.22] Manipulación de programas</p> <p>[A.23] Manipulación del hardware</p> <p>[A.24] Denegación de servicio</p> <p>[A.25] Robo de equipos</p> <p>[A.26] Ataque destructivo</p> <p>[A.28] Indisponibilidad del personal</p> <p>[A.29] Extorsión</p> <p>[A.30] Ingeniería social (picaresca)</p> <p>Total</p> <p>[N.1] Fuego</p> <p>[N.2] Daños por agua</p> <p>[N.*] Desastres naturales</p> <p>[I.1] Fuego</p> <p>[I.2] Daños por agua</p> <p>[I.*] Desastres industriales</p> <p>[I.3] Contaminación medioambiental</p> <p>[I.4] Contaminación electromagnética</p> <p>[I.5] Avería de origen físico o lógico</p> <p>[I.6] Corte del suministro eléctrico</p> <p>[I.7] Condiciones inadecuadas de temperatura o humedad</p> <p>[E.15] Alteración de la información</p> <p>[E.19] Fugas de información</p> <p>[E.23] Errores de mantenimiento / actualización de equipos (hardware)</p> <p>[E.24] Caída del sistema por agotamiento de los recursos</p> <p>[E.25] Pérdida de equipos</p> <p>[E.28] Indisponibilidad del personal</p> <p>[A.7] Uso no previsto</p> <p>[A.11] Acceso no autorizado</p> <p>[A.15] Modificación de la información</p> <p>[A.18] Destrucción de la información</p> <p>[A.19] Revelación de información</p> <p>[A.23] Manipulación del hardware</p> <p>[A.24] Denegación de servicio</p> <p>[A.25] Robo de equipos</p> <p>[A.26] Ataque destructivo</p> <p>[A.28] Indisponibilidad del personal</p> <p>[A.29] Extorsión</p> <p>[A.30] Ingeniería social (picaresca)</p> <p>Total</p> <p>[N.1] Fuego</p> <p>[N.2] Daños por agua</p> <p>[N.*] Desastres naturales</p> <p>[I.1] Fuego</p>
[HW-SW] SWITCH	<p>[E.15] Alteración de la información</p> <p>[E.19] Fugas de información</p> <p>[E.23] Errores de mantenimiento / actualización de equipos (hardware)</p> <p>[E.24] Caída del sistema por agotamiento de los recursos</p> <p>[E.25] Pérdida de equipos</p> <p>[E.28] Indisponibilidad del personal</p> <p>[A.7] Uso no previsto</p> <p>[A.11] Acceso no autorizado</p> <p>[A.15] Modificación de la información</p> <p>[A.18] Destrucción de la información</p> <p>[A.19] Revelación de información</p> <p>[A.23] Manipulación del hardware</p> <p>[A.24] Denegación de servicio</p> <p>[A.25] Robo de equipos</p> <p>[A.26] Ataque destructivo</p> <p>[A.28] Indisponibilidad del personal</p> <p>[A.29] Extorsión</p> <p>[A.30] Ingeniería social (picaresca)</p> <p>Total</p> <p>[N.1] Fuego</p> <p>[N.2] Daños por agua</p> <p>[N.*] Desastres naturales</p> <p>[I.1] Fuego</p>
[HW-CT] CENTRAL IP	<p>[N.1] Fuego</p> <p>[N.2] Daños por agua</p> <p>[N.*] Desastres naturales</p> <p>[I.1] Fuego</p>

**[HW-TM]
TELEFONIA
MOVIL**

[I.2] Daños por agua
[I.*] Desastres industriales
[I.3] Contaminación medioambiental
[I.4] Contaminación electromagnética
[I.5] Avería de origen físico o lógico
[I.6] Corte del suministro eléctrico
[I.7] Condiciones inadecuadas de temperatura o humedad
[E.1] Errores de los usuarios
[E.2] Errores del administrador del sistema / de la seguridad
[E.15] Alteración de la información
[E.18] Destrucción de la información
[E.19] Fugas de información
[E.23] Errores de mantenimiento / actualización de equipos (hardware)
[E.24] Caída del sistema por agotamiento de los recursos
[E.25] Pérdida de equipos
[E.28] Indisponibilidad del personal
[A.5] Suplantación de la identidad
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.11] Acceso no autorizado
[A.13] Repudio (negación de actuaciones)
[A.15] Modificación de la información
[A.18] Destrucción de la información
[A.19] Revelación de información
[A.23] Manipulación del hardware
[A.24] Denegación de servicio
[A.25] Robo de equipos
[A.26] Ataque destructivo
[A.28] Indisponibilidad del personal
[A.29] Extorsión
[A.30] Ingeniería social (picaresca)
Total
[N.1] Fuego
[N.2] Daños por agua
[N.*] Desastres naturales
[I.1] Fuego
[I.2] Daños por agua
[I.*] Desastres industriales
[I.3] Contaminación medioambiental
[I.4] Contaminación electromagnética
[I.5] Avería de origen físico o lógico
[I.6] Corte del suministro eléctrico
[I.7] Condiciones inadecuadas de temperatura o humedad
[E.1] Errores de los usuarios
[E.2] Errores del administrador del sistema / de la seguridad

**[HW-FIRE]
FIREWALL**

[E.15] Alteración de la información
[E.18] Destrucción de la información
[E.19] Fugas de información
[E.23] Errores de mantenimiento / actualización de equipos (hardware)
[E.24] Caída del sistema por agotamiento de los recursos
[E.25] Pérdida de equipos
[E.28] Indisponibilidad del personal
[A.5] Suplantación de la identidad
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.11] Acceso no autorizado
[A.15] Modificación de la información
[A.18] Destrucción de la información
[A.19] Revelación de información
[A.23] Manipulación del hardware
[A.24] Denegación de servicio
[A.25] Robo de equipos
[A.26] Ataque destructivo
[A.28] Indisponibilidad del personal
[A.29] Extorsión
[A.30] Ingeniería social (picaresca)
Total
[N.1] Fuego
[N.2] Daños por agua
[N.*] Desastres naturales
[I.1] Fuego
[I.2] Daños por agua
[I.*] Desastres industriales
[I.3] Contaminación medioambiental
[I.4] Contaminación electromagnética
[I.5] Avería de origen físico o lógico
[I.6] Corte del suministro eléctrico
[I.7] Condiciones inadecuadas de temperatura o humedad
[E.15] Alteración de la información
[E.19] Fugas de información
[E.23] Errores de mantenimiento / actualización de equipos (hardware)
[E.24] Caída del sistema por agotamiento de los recursos
[E.25] Pérdida de equipos
[E.28] Indisponibilidad del personal
[A.7] Uso no previsto
[A.11] Acceso no autorizado
[A.15] Modificación de la información
[A.18] Destrucción de la información
[A.19] Revelación de información
[A.23] Manipulación del hardware

	<ul style="list-style-type: none"> [A.24] Denegación de servicio [A.25] Robo de equipos [A.26] Ataque destructivo [A.28] Indisponibilidad del personal [A.29] Extorsión [A.30] Ingeniería social (picaresca) Total [I.8] Fallo de servicios de comunicaciones [E.2] Errores del administrador del sistema / de la seguridad [E.9] Errores de [re-]encaminamiento [E.10] Errores de secuencia [E.15] Alteración de la información [E.19] Fugas de información [E.24] Caída del sistema por agotamiento de los recursos [E.28] Indisponibilidad del personal
[COM-LAN] RED LAN	<ul style="list-style-type: none"> [A.5] Suplantación de la identidad [A.7] Uso no previsto [A.9] [Re-]encaminamiento de mensajes [A.10] Alteración de secuencia [A.11] Acceso no autorizado [A.15] Modificación de la información [A.18] Destrucción de la información [A.19] Revelación de información [A.24] Denegación de servicio [A.28] Indisponibilidad del personal [A.29] Extorsión [A.30] Ingeniería social (picaresca) Total [I.8] Fallo de servicios de comunicaciones [E.2] Errores del administrador del sistema / de la seguridad [E.9] Errores de [re-]encaminamiento [E.10] Errores de secuencia [E.15] Alteración de la información [E.18] Destrucción de la información [E.19] Fugas de información [E.24] Caída del sistema por agotamiento de los recursos [E.28] Indisponibilidad del personal
[COM] COMUNICACIONES	<ul style="list-style-type: none"> [A.5] Suplantación de la identidad [A.7] Uso no previsto [A.9] [Re-]encaminamiento de mensajes [A.10] Alteración de secuencia [A.11] Acceso no autorizado [A.13] Repudio (negación de actuaciones) [A.14] Interceptación de información (escucha) [A.15] Modificación de la información [A.18] Destrucción de la información
[COM-FO] FIBRA OPTICA	<ul style="list-style-type: none"> [A.5] Suplantación de la identidad [A.7] Uso no previsto [A.9] [Re-]encaminamiento de mensajes [A.10] Alteración de secuencia [A.11] Acceso no autorizado [A.13] Repudio (negación de actuaciones) [A.14] Interceptación de información (escucha) [A.15] Modificación de la información [A.18] Destrucción de la información

		<p>[A.19] Revelación de información</p> <p>[A.24] Denegación de servicio</p> <p>[A.28] Indisponibilidad del personal</p> <p>[A.29] Extorsión</p> <p>[A.30] Ingeniería social (picaresca)</p> <p>Total</p> <p>[I.8] Fallo de servicios de comunicaciones</p> <p>[E.2] Errores del administrador del sistema / de la seguridad</p> <p>[E.9] Errores de [re-]encaminamiento</p> <p>[E.10] Errores de secuencia</p> <p>[E.15] Alteración de la información</p> <p>[E.18] Destrucción de la información</p> <p>[E.19] Fugas de información</p> <p>[E.24] Caída del sistema por agotamiento de los recursos</p> <p>[E.28] Indisponibilidad del personal</p> <p>[A.5] Suplantación de la identidad</p> <p>[A.7] Uso no previsto</p> <p>[A.9] [Re-]encaminamiento de mensajes</p> <p>[A.10] Alteración de secuencia</p> <p>[A.11] Acceso no autorizado</p> <p>[A.13] Repudio (negación de actuaciones)</p> <p>[A.14] Interceptación de información (escucha)</p> <p>[A.15] Modificación de la información</p> <p>[A.18] Destrucción de la información</p> <p>[A.19] Revelación de información</p> <p>[A.24] Denegación de servicio</p> <p>[A.28] Indisponibilidad del personal</p> <p>[A.29] Extorsión</p> <p>[A.30] Ingeniería social (picaresca)</p> <p>Total</p> <p>[I.8] Fallo de servicios de comunicaciones</p> <p>[E.2] Errores del administrador del sistema / de la seguridad</p> <p>[E.24] Caída del sistema por agotamiento de los recursos</p> <p>[E.28] Indisponibilidad del personal</p> <p>[A.5] Suplantación de la identidad</p> <p>[A.7] Uso no previsto</p> <p>[A.11] Acceso no autorizado</p> <p>[A.18] Destrucción de la información</p> <p>[A.24] Denegación de servicio</p> <p>[A.28] Indisponibilidad del personal</p> <p>[A.29] Extorsión</p> <p>[A.30] Ingeniería social (picaresca)</p> <p>Total</p> <p>[N.1] Fuego</p> <p>[N.2] Daños por agua</p> <p>[N.*] Desastres naturales</p>
	[COM-VPN] CONEXIÓN VPN	
	[COM-WIFI] RED INALAMBRICA	
[AUX] ELEMENTOS AUXILIARES	[AUX-FA] FUENTES DE ALIMENTACION	

	<ul style="list-style-type: none"> [I.1] Fuego [I.2] Daños por agua [I.*] Desastres industriales [I.3] Contaminación medioambiental [E.23] Errores de mantenimiento / actualización de equipos (hardware) [E.28] Indisponibilidad del personal [A.7] Uso no previsto [A.18] Destrucción de la información [A.23] Manipulación del hardware [A.25] Robo de equipos [A.26] Ataque destructivo [A.28] Indisponibilidad del personal [A.29] Extorsión [A.30] Ingeniería social (picaresca) Total [N.1] Fuego [N.2] Daños por agua [N.*] Desastres naturales [I.1] Fuego [I.2] Daños por agua [I.*] Desastres industriales [I.3] Contaminación medioambiental [E.15] Alteración de la información [E.19] Fugas de información [E.23] Errores de mantenimiento / actualización de equipos (hardware) [A.7] Uso no previsto [A.15] Modificación de la información [A.18] Destrucción de la información [A.19] Revelación de información [A.23] Manipulación del hardware [A.25] Robo de equipos [A.26] Ataque destructivo [A.28] Indisponibilidad del personal [A.29] Extorsión [A.30] Ingeniería social (picaresca) Total [N.1] Fuego [N.2] Daños por agua [N.*] Desastres naturales [I.1] Fuego [I.2] Daños por agua [I.*] Desastres industriales [I.3] Contaminación medioambiental [I.6] Corte del suministro eléctrico [I.9] Interrupción de otros servicios o suministros esenciales [E.23] Errores de mantenimiento / actualización de equipos (hardware)
[AUX-CCTV] SISTEMA DE CCTV	
[AUX-AA] AIRE ACONDICIONADO	

		<ul style="list-style-type: none"> [E.28] Indisponibilidad del personal [A.7] Uso no previsto [A.18] Destrucción de la información [A.23] Manipulación del hardware [A.25] Robo de equipos [A.26] Ataque destructivo [A.28] Indisponibilidad del personal [A.29] Extorsión [A.30] Ingeniería social (picaresca) Total
	[AUX-UPS] UPS	<ul style="list-style-type: none"> [E.28] Indisponibilidad del personal [A.18] Destrucción de la información [A.28] Indisponibilidad del personal [A.29] Extorsión [A.30] Ingeniería social (picaresca) Total
	[AUX-GE] GRUPO ELECTROGENO	<ul style="list-style-type: none"> [E.28] Indisponibilidad del personal [A.18] Destrucción de la información [A.28] Indisponibilidad del personal [A.29] Extorsión [A.30] Ingeniería social (picaresca) Total
	[AUX-CD] CABLEADO DE DATOS	<ul style="list-style-type: none"> [N.1] Fuego [N.2] Daños por agua [N.*] Desastres naturales [I.1] Fuego [I.2] Daños por agua [I.*] Desastres industriales [I.3] Contaminación medioambiental [I.4] Contaminación electromagnética [E.23] Errores de mantenimiento / actualización de equipos (hardware) [E.28] Indisponibilidad del personal [A.7] Uso no previsto [A.18] Destrucción de la información [A.23] Manipulación del hardware [A.25] Robo de equipos [A.26] Ataque destructivo [A.28] Indisponibilidad del personal [A.29] Extorsión [A.30] Ingeniería social (picaresca) Total
[L] INSTALACIONES	[L-ARQ] DATA CENTER OFICINA AREQUIPA	<ul style="list-style-type: none"> [N.1] Fuego [N.2] Daños por agua [N.*] Desastres naturales [I.1] Fuego [I.2] Daños por agua [I.*] Desastres industriales [I.3] Contaminación medioambiental

		<ul style="list-style-type: none"> [I.4] Contaminación electromagnética [E.15] Alteración de la información [E.19] Fugas de información [E.28] Indisponibilidad del personal [A.6] Abuso de privilegios de acceso [A.7] Uso no previsto [A.15] Modificación de la información [A.18] Destrucción de la información [A.19] Revelación de información [A.26] Ataque destructivo [A.27] Ocupación enemiga [A.28] Indisponibilidad del personal [A.29] Extorsión [A.30] Ingeniería social (picaresca) Total [N.1] Fuego [N.2] Daños por agua [N.*] Desastres naturales [I.1] Fuego [I.2] Daños por agua [I.*] Desastres industriales [I.3] Contaminación medioambiental [I.4] Contaminación electromagnética
	[L-SC] DATA CENTER OFICINA SANTA CRUZ	<ul style="list-style-type: none"> [E.15] Alteración de la información [E.19] Fugas de información [E.28] Indisponibilidad del personal [A.6] Abuso de privilegios de acceso [A.7] Uso no previsto [A.15] Modificación de la información [A.18] Destrucción de la información [A.19] Revelación de información [A.26] Ataque destructivo [A.27] Ocupación enemiga [A.28] Indisponibilidad del personal [A.29] Extorsión [A.30] Ingeniería social (picaresca) Total
[P] PERSONAL	[P-AIT] PERSONAL ADMINISTRACION IT	<ul style="list-style-type: none"> [E.15] Alteración de la información [E.19] Fugas de información [E.28] Indisponibilidad del personal [A.5] Suplantación de la identidad [A.6] Abuso de privilegios de acceso [A.11] Acceso no autorizado [A.15] Modificación de la información [A.18] Destrucción de la información [A.19] Revelación de información [A.28] Indisponibilidad del personal [A.29] Extorsión [A.30] Ingeniería social (picaresca)

	Total
	[E.15] Alteración de la información
	[E.19] Fugas de información
	[E.28] Indisponibilidad del personal
	[A.5] Suplantación de la identidad
[P-DIT]	[A.6] Abuso de privilegios de acceso
PERSONAL	[A.11] Acceso no autorizado
DESARROLLO IT	[A.15] Modificación de la información
	[A.18] Destrucción de la información
	[A.19] Revelación de información
	[A.28] Indisponibilidad del personal
	[A.29] Extorsión
	[A.30] Ingeniería social (picaresca)

Nota: Elaboración propia.

ANEXO N° 9 VALORACION DE AMENAZAS

Tabla 69.

Valoración de amenazas

ACTIVOS	AMENAZAS	PROB ABILI DAD	[D]	[I]	[C]	[A]	[T]
	Total		10	10	10	10	10
	[I.5] Avería de origen físico o lógico	P	5				
	[E.1] Errores de los usuarios	P	1	1	1		
	[E.2] Errores del administrador del sistema / de la seguridad	P	2	2	2		
	[E.8] Difusión de software dañino	P	1	1	1		
	[E.15] Alteración de la información	P		1			
	[E.18] Destrucción de la información	P	1				
	[E.19] Fugas de información	P			1		
	[E.20] Vulnerabilidades de los programas (software)	P	0	2	2		
	[E.24] Caída del sistema por agotamiento de los recursos	MA	5				
[SG- SISGECO] SISTEMA DE GESTIÓN SISGECO	[E.28] Indisponibilidad del personal	P	2				
	[A.5] Suplantación de la identidad	CS		5	5	10	
	[A.6] Abuso de privilegios de acceso	CS	0	1	5	10	
	[A.7] Uso no previsto	MA	0	1	1		
	[A.8] Difusión de software dañino	MA	10	10	10		
	[A.11] Acceso no autorizado	CS		1	5	10	
	[A.13] Repudio (negación de actuaciones)	MA					10
	[A.15] Modificación de la información	CS		5			
	[A.18] Destrucción de la información	MA	5				
	[A.19] Revelación de información	CS			5		
	[A.22] Manipulación de programas	MA	5	10	10		
	[A.24] Denegación de servicio	CS	5				
	[A.28] Indisponibilidad del personal	P	5				
	[A.29] Extorsión	MA	5	10	10		
	[A.30] Ingeniería social (picaresca)	P	5	10	10		
	Total		10	10	10	10	10
	[I.5] Avería de origen físico o lógico	P	5				
	[E.1] Errores de los usuarios	P	1	1	1		
	[E.2] Errores del administrador del sistema / de la seguridad	P	2	2	2		
[SW-SSP] SOFTWARE E STAR SOFT PLANILLAS	[E.8] Difusión de software dañino	P	1	1	1		
	[E.15] Alteración de la información	P		1			
	[E.18] Destrucción de la información	P	1				
	[E.19] Fugas de información	P			1		
	[E.20] Vulnerabilidades de los programas (software)	P	0	2	2		
	[E.24] Caída del sistema por agotamiento de los recursos	MA	5				
	[E.28] Indisponibilidad del personal	P	2				
	[A.5] Suplantación de la identidad	CS		5	5	10	

	[A.6] Abuso de privilegios de acceso	CS	0	1	5	10		
	[A.7] Uso no previsto	MA	0	1	1			
	[A.8] Difusión de software dañino	MA	10	10	10			
	[A.11] Acceso no autorizado	CS		1	5	10		
	[A.13] Repudio (negación de actuaciones)	MA						10
	[A.15] Modificación de la información	CS		5				
	[A.18] Destrucción de la información	MA	5					
	[A.19] Revelación de información	CS			5			
	[A.22] Manipulación de programas	MA	5	10	10			
	[A.24] Denegación de servicio	CS	5					
	[A.28] Indisponibilidad del personal	P	5					
	[A.29] Extorsión	MA	5	10	10			
	[A.30] Ingeniería social (picaresca)	P	5	10	10			
	Total		10	10	10	10	10	10
	[I.5] Avería de origen físico o lógico	P	5					
	[E.1] Errores de los usuarios	P	1	1	1			
	[E.2] Errores del administrador del sistema / de la seguridad	P	2	2	2			
	[E.8] Difusión de software dañino	P	1	1	1			
	[E.15] Alteración de la información	P		1				
	[E.18] Destrucción de la información	P	1					
	[E.19] Fugas de información	P			1			
	[E.20] Vulnerabilidades de los programas (software)	P	0	2	2			
	[E.24] Caída del sistema por agotamiento de los recursos	MA	5					
	[E.28] Indisponibilidad del personal	P	2					
[SW- SISCONT] SOFTWARE E SISCONT	[A.5] Suplantación de la identidad	CS		5	5	10		
	[A.6] Abuso de privilegios de acceso	CS	0	1	5	10		
	[A.7] Uso no previsto	MA	0	1	1			
	[A.8] Difusión de software dañino	MA	10	10	10			
	[A.11] Acceso no autorizado	CS		1	5	10		
	[A.13] Repudio (negación de actuaciones)	MA						10
	[A.15] Modificación de la información	CS		5				
	[A.18] Destrucción de la información	MA	5					
	[A.19] Revelación de información	CS			5			
	[A.22] Manipulación de programas	MA	5	10	10			
	[A.24] Denegación de servicio	CS	5					
	[A.28] Indisponibilidad del personal	P	5					
	[A.29] Extorsión	MA	5	10	10			
	[A.30] Ingeniería social (picaresca)	P	5	10	10			
	Total		10	10	10	10	10	10
[SW-GBD] SISTEMA DE GESTION DE BASE DE DATOS	[I.5] Avería de origen físico o lógico	P	5					
	[E.1] Errores de los usuarios	P	1	1	1			
	[E.2] Errores del administrador del sistema / de la seguridad	P	2	2	2			
	[E.8] Difusión de software dañino	P	1	1	1			
	[E.15] Alteración de la información	P		1				

[E.18] Destrucción de la información	P	1				
[E.19] Fugas de información	P			1		
[E.20] Vulnerabilidades de los programas (software)	P	0	2	2		
[E.24] Caída del sistema por agotamiento de los recursos	MA	5				
[E.28] Indisponibilidad del personal	P	3				
[A.5] Suplantación de la identidad	MA		5	5	10	
[A.6] Abuso de privilegios de acceso	MA	0	1	1	10	
[A.7] Uso no previsto	MA	0	1	1		
[A.8] Difusión de software dañino	MA	10	10	10		
[A.11] Acceso no autorizado	MA		1	5	10	
[A.13] Repudio (negación de actuaciones)	MA					10
[A.15] Modificación de la información	CS		5			
[A.18] Destrucción de la información	MA	5				
[A.19] Revelación de información	CS			5		
[A.22] Manipulación de programas	MA	5	10	10		
[A.24] Denegación de servicio	CS	5				
[A.28] Indisponibilidad del personal	P	5				
[A.29] Extorsión	MA	5	10	10		
[A.30] Ingeniería social (picaresca)	P	5	10	10		
Total		10	10	10	10	10
[I.5] Avería de origen físico o lógico	P	5				
[E.1] Errores de los usuarios	P	1	1	1		
[E.2] Errores del administrador del sistema / de la seguridad	P	2	2	2		
[E.8] Difusión de software dañino	P	1	1	1		
[E.15] Alteración de la información	P		1			
[E.18] Destrucción de la información	P	1				
[E.19] Fugas de información	P			1		
[E.20] Vulnerabilidades de los programas (software)	P	0	2	2		
[E.24] Caída del sistema por agotamiento de los recursos	MA	5				
[E.28] Indisponibilidad del personal	P	2				
[SW- INTRANET] SISTEMA INTRANET	[A.5] Suplantación de la identidad	MA		5	5	10
	[A.6] Abuso de privilegios de acceso	MA	0	1	1	
	[A.7] Uso no previsto	MA	0	1	1	
	[A.8] Difusión de software dañino	MA	10	10	10	
	[A.11] Acceso no autorizado	MA		1	5	10
	[A.13] Repudio (negación de actuaciones)	MA				10
	[A.15] Modificación de la información	CS		5		
	[A.18] Destrucción de la información	MA	5			
	[A.19] Revelación de información	CS			5	
	[A.22] Manipulación de programas	MA	5	10	10	
	[A.24] Denegación de servicio	CS	5			
	[A.28] Indisponibilidad del personal	P	5			
	[A.29] Extorsión	MA	5	10	10	
	[A.30] Ingeniería social (picaresca)	P	5	10	10	

	Total		10	10	10		
	[I.5] Avería de origen físico o lógico	P	5				
	[E.8] Difusión de software dañino	P	1	1	1		
	[E.15] Alteración de la información	P		1			
	[E.19] Fugas de información	P			1		
[SW-ANTIVIRUS]	[E.20] Vulnerabilidades de los programas (software)	P	0	2	2		
ANTIVIRUS	[E.28] Indisponibilidad del personal	P	3				
BITDEFENDER	[A.8] Difusión de software dañino	MA	10	10	10		
	[A.15] Modificación de la información	MA		5			
	[A.18] Destrucción de la información	MA	1				
	[A.19] Revelación de información	CS			5		
	[A.22] Manipulación de programas	MA	5	10	10		
	[A.28] Indisponibilidad del personal	P	5				
	[A.29] Extorsión	MA	5	10	10	10	
	[A.30] Ingeniería social (picaresca)	P	5	10	10		
	Total		10	10	10	10	10
	[I.5] Avería de origen físico o lógico	P	5				
	[E.1] Errores de los usuarios	P	1	1	1		
	[E.2] Errores del administrador del sistema / de la seguridad	P	2	2	2		
	[E.8] Difusión de software dañino	P	1	1	1		
	[E.15] Alteración de la información	P		1			
	[E.18] Destrucción de la información	P	1				
	[E.19] Fugas de información	P			1		
	[E.20] Vulnerabilidades de los programas (software)	P	0	2	2		
	[E.24] Caída del sistema por agotamiento de los recursos	MA	5				
	[E.28] Indisponibilidad del personal	P	3				
[SW-SO]	[A.5] Suplantación de la identidad	MA		5	5	10	
SISTEMA	[A.6] Abuso de privilegios de acceso	MA	0	1	1	10	
OPERATIVO	[A.7] Uso no previsto	MA	0	1	1		
O	[A.8] Difusión de software dañino	MA	10	10	10		
	[A.11] Acceso no autorizado	MA		1	5	10	
	[A.13] Repudio (negación de actuaciones)	MA					10
	[A.15] Modificación de la información	CS		5			
	[A.18] Destrucción de la información	MA	5				
	[A.19] Revelación de información	CS			5		
	[A.22] Manipulación de programas	MA	5	10	10		
	[A.24] Denegación de servicio	CS	5				
	[A.28] Indisponibilidad del personal	P	5				
	[A.29] Extorsión	MA	5	10	10		
	[A.30] Ingeniería social (picaresca)	P	5	10	10		
	Total		1	10	10		
[SW-OF]	[E.8] Difusión de software dañino	P	0	1	1		
OFIMATICA	[E.15] Alteración de la información	P	0	1			
	[E.19] Fugas de información	P	0		1		

	[E.20] Vulnerabilidades de los programas (software)	P	0	2	2		
	[A.8] Difusión de software dañino	MA	1	10	10		
	[A.15] Modificación de la información	MA	0	5			
	[A.19] Revelación de información	CS	0		5		
	[A.22] Manipulación de programas	MA	0	10	10		
	[A.29] Extorsión	MA	0	10	10		
	[A.30] Ingeniería social (picaresca)	P	0	10	10		
	Total		10	10	10	10	10
	[N.1] Fuego	PP	10				
	[N.2] Daños por agua	PP	1				
	[N.*] Desastres naturales	PP	10				
	[I.1] Fuego	P	10				
	[I.2] Daños por agua	P	5				
	[I.*] Desastres industriales	P	10				
	[I.3] Contaminación medioambiental	P	5				
	[I.4] Contaminación electromagnética	P	5				
	[I.5] Avería de origen físico o lógico	P	10				
	[I.6] Corte del suministro eléctrico	P	10				
	[I.7] Condiciones inadecuadas de temperatura o humedad	P	10				
	[I.10] Degradación de los soportes de almacenamiento de la información	P	10				
	[E.1] Errores de los usuarios	P	1	1	1		
	[E.2] Errores del administrador del sistema / de la seguridad	P	2	2	2		
[BCK] BACKUPS	[E.18] Destrucción de la información	P	10				
	[E.19] Fugas de información	P				1	
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	P	10				
	[E.24] Caída del sistema por agotamiento de los recursos	MA	5				
	[E.25] Pérdida de equipos	P	10		5		
	[A.5] Suplantación de la identidad	CS		5	5	10	
	[A.6] Abuso de privilegios de acceso	CS	0	1	5	10	
	[A.7] Uso no previsto	MA	0	1	1	1	
	[A.11] Acceso no autorizado	CS	1	1	5	10	
	[A.13] Repudio (negación de actuaciones)	MA					10
	[A.15] Modificación de la información	CS		10			
	[A.18] Destrucción de la información	MA	10				
	[A.23] Manipulación del hardware	P	5		5		
	[A.24] Denegación de servicio	CS	10				
	[A.25] Robo de equipos	MA	10		10		
	[A.26] Ataque destructivo	MA	10				
	Total		10	10	10	10	10
[SW-CC] CORREO CORPORA TIVO	[I.5] Avería de origen físico o lógico	P	5				
	[I.9] Interrupción de otros servicios o suministros esenciales	P	5				
	[E.8] Difusión de software dañino	P	1	1	1		
	[E.15] Alteración de la información	P		1			

[E.18] Destrucción de la información	P	1			
[E.19] Fugas de información	P			1	
[E.20] Vulnerabilidades de los programas (software)	P	0	2	2	
[E.28] Indisponibilidad del personal	P	3			
[A.5] Suplantación de la identidad	CS		10	10	10
[A.6] Abuso de privilegios de acceso	CS	0	1	5	
[A.8] Difusión de software dañino	MA	10	10	10	
[A.11] Acceso no autorizado	CS		1	5	
[A.13] Repudio (negación de actuaciones)	MA				10
[A.15] Modificación de la información	MA		5		
[A.18] Destrucción de la información	MA	5			
[A.19] Revelación de información	CS			5	
[A.22] Manipulación de programas	MA	5	10	10	
[A.24] Denegación de servicio	MA	5			
[A.28] Indisponibilidad del personal	P	5			
[A.29] Extorsión	MA	5	10	10	
[A.30] Ingeniería social (picaresca)	P	5	10	10	
Total		10	10	10	10
[N.1] Fuego	PP	10			
[N.2] Daños por agua	PP	5			
[N.*] Desastres naturales	PP	10			
[I.1] Fuego	P	10			
[I.2] Daños por agua	P	5			
[I.*] Desastres industriales	P	10			
[I.3] Contaminación medioambiental	PP	5			
[I.4] Contaminación electromagnética	P	1			
[I.5] Avería de origen físico o lógico	P	5			
[I.6] Corte del suministro eléctrico	P	10			
[I.7] Condiciones inadecuadas de temperatura o humedad	P	10			
[HW-SBD] [E.8] Difusión de software dañino	P	1	1	1	
SERVIDOR [E.15] Alteración de la información	P		1		
DE BASE [E.19] Fugas de información	P			1	
DE DATOS [E.20] Vulnerabilidades de los programas (software)	P	0	2	2	
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	P	1			
[E.24] Caída del sistema por agotamiento de los recursos	MA	5			
[E.25] Pérdida de equipos	PP	10		10	
[E.28] Indisponibilidad del personal	P	2			
[A.5] Suplantación de la identidad	CS		1	5	10
[A.6] Abuso de privilegios de acceso	CS	0	1	5	
[A.7] Uso no previsto	MA	0	0	1	
[A.8] Difusión de software dañino	MA	10	10	10	
[A.11] Acceso no autorizado	CS	1	1	5	
[A.15] Modificación de la información	MA		5		

	[A.18] Destrucción de la información	MA	1				
	[A.19] Revelación de información	CS			5		
	[A.22] Manipulación de programas	MA	5	10	10		
	[A.23] Manipulación del hardware	P	5		5		
	[A.24] Denegación de servicio	MA	10				
	[A.25] Robo de equipos	P	10		10		
	[A.26] Ataque destructivo	MA	10				
	[A.28] Indisponibilidad del personal	P	2				
	[A.29] Extorsión	MA	5	10	10		
	[A.30] Ingeniería social (picaresca)	P	5	10	10		
	Total			10	10	10	10 10
	[N.1] Fuego	PP	10				
	[N.2] Daños por agua	PP	5				
	[N.*] Desastres naturales	PP	10				
	[I.1] Fuego	P	10				
	[I.2] Daños por agua	P	5				
	[I.*] Desastres industriales	P	10				
	[I.3] Contaminación medioambiental	PP	5				
	[I.4] Contaminación electromagnética	P	1				
	[I.5] Avería de origen físico o lógico	P	5				
	[I.6] Corte del suministro eléctrico	P	10				
	[I.7] Condiciones inadecuadas de temperatura o humedad	P	10				
	[E.1] Errores de los usuarios	P	1	1	1		
	[E.2] Errores del administrador del sistema / de la seguridad	P	2	2	2		
	[E.8] Difusión de software dañino	P	1	1	1		
[HW-PC]	[E.15] Alteración de la información	P		1			
COMPUTA	[E.18] Destrucción de la información	P	1				
DORA DE	[E.19] Fugas de información	P			1		
ESCRITORI	[E.20] Vulnerabilidades de los programas (software)	P	0	2	2		
O	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	P	1				
	[E.24] Caída del sistema por agotamiento de los recursos	MA	5				
	[E.25] Pérdida de equipos	MA	0		1		
	[E.28] Indisponibilidad del personal	P	1				
	[A.5] Suplantación de la identidad	CS		5	5	10	
	[A.6] Abuso de privilegios de acceso	CS	0	1	5	10	
	[A.7] Uso no previsto	MA	1	1	1		
	[A.8] Difusión de software dañino	MA	10	10	10		
	[A.11] Acceso no autorizado	CS	1	1	5	10	
	[A.13] Repudio (negación de actuaciones)	MA					10
	[A.15] Modificación de la información	CS		5			
	[A.18] Destrucción de la información	MA	5				
	[A.19] Revelación de información	CS			2		
	[A.22] Manipulación de programas	MA	5	10	10		

	[A.23] Manipulación del hardware	P	5	5		
	[A.24] Denegación de servicio	CS	10			
	[A.25] Robo de equipos	MA	0	1		
	[A.26] Ataque destructivo	MA	10			
	[A.28] Indisponibilidad del personal	P	5			
	[A.29] Extorsión	MA	1	2	2	
	[A.30] Ingeniería social (picaresca)	P	1	2	2	
	Total					
	[N.1] Fuego	PP	10			
	[N.2] Daños por agua	PP	5			
	[N.*] Desastres naturales	PP	10			
	[I.1] Fuego	P	10			
	[I.2] Daños por agua	P	5			
	[I.*] Desastres industriales	P	10			
	[I.3] Contaminación medioambiental	PP	5			
	[I.4] Contaminación electromagnética	P	1			
	[I.5] Avería de origen físico o lógico	P	5			
	[I.6] Corte del suministro eléctrico	P	10			
	[I.7] Condiciones inadecuadas de temperatura o humedad	P	10			
	[E.1] Errores de los usuarios	P	1			
	[E.2] Errores del administrador del sistema / de la seguridad	P	2			
	[E.18] Destrucción de la información	P	1			
	[E.19] Fugas de información	P			1	
[HW-IMP] IMPRESOR AS	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	P	1			
	[E.24] Caída del sistema por agotamiento de los recursos	MA	5			
	[E.25] Pérdida de equipos	P	10	5		
	[E.28] Indisponibilidad del personal	P	1			
	[A.5] Suplantación de la identidad	CS		5	10	
	[A.6] Abuso de privilegios de acceso	CS	0	5	10	
	[A.7] Uso no previsto	MA	0	1		
	[A.11] Acceso no autorizado	CS	1	5	10	
	[A.18] Destrucción de la información	MA	5			
	[A.19] Revelación de información	CS		2		
	[A.23] Manipulación del hardware	P	5	5		
	[A.24] Denegación de servicio	CS	10			
	[A.25] Robo de equipos	P	10	5		
	[A.26] Ataque destructivo	MA	10			
	[A.28] Indisponibilidad del personal	P	5			
	[A.29] Extorsión	MA	1	2		
	[A.30] Ingeniería social (picaresca)	P	1	2		
[HW-AP] SERVIDOR APLICACIONES	Total		10	10	10	10
	[N.1] Fuego	PP	10			
	[N.2] Daños por agua	PP	5			

	[N.*] Desastres naturales	PP	10			
	[I.1] Fuego	P	10			
	[I.2] Daños por agua	P	5			
	[I.*] Desastres industriales	P	10			
	[I.3] Contaminación medioambiental	PP	5			
	[I.4] Contaminación electromagnética	P	1			
	[I.5] Avería de origen físico o lógico	P	5			
	[I.6] Corte del suministro eléctrico	P	10			
	[I.7] Condiciones inadecuadas de temperatura o humedad	P	10			
	[E.8] Difusión de software dañino	P	1	1	1	
	[E.15] Alteración de la información	P		1		
	[E.19] Fugas de información	P			1	
	[E.20] Vulnerabilidades de los programas (software)	P	0	2	2	
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	P	1			
	[E.24] Caída del sistema por agotamiento de los recursos	MA	5			
	[E.25] Pérdida de equipos	PP	10		10	
	[E.28] Indisponibilidad del personal	P	1			
	[A.5] Suplantación de la identidad	CS		1	5	10
	[A.6] Abuso de privilegios de acceso	CS	0	1	5	
	[A.7] Uso no previsto	MA	0	0	1	
	[A.8] Difusión de software dañino	MA	10	10	10	
	[A.11] Acceso no autorizado	CS	1	1	5	
	[A.15] Modificación de la información	MA		5		
	[A.18] Destrucción de la información	MA	1			
	[A.19] Revelación de información	CS			2	
	[A.22] Manipulación de programas	MA	5	10	10	
	[A.23] Manipulación del hardware	P	5		5	
	[A.24] Denegación de servicio	MA	10			
	[A.25] Robo de equipos	P	10		10	
	[A.26] Ataque destructivo	MA	10			
	[A.28] Indisponibilidad del personal	P	5			
	[A.29] Extorsión	MA	1	2	2	
	[A.30] Ingeniería social (picaresca)	P	1	2	2	
	Total		10	5	5	
	[N.1] Fuego	PP	10			
	[N.2] Daños por agua	PP	5			
	[N.*] Desastres naturales	PP	10			
[HW-SW] SWITCH	[I.1] Fuego	P	10			
	[I.2] Daños por agua	P	5			
	[I.*] Desastres industriales	P	10			
	[I.3] Contaminación medioambiental	PP	5			
	[I.4] Contaminación electromagnética	P	1			
	[I.5] Avería de origen físico o lógico	P	5			

[I.6] Corte del suministro eléctrico	P	10				
[I.7] Condiciones inadecuadas de temperatura o humedad	P	10				
[E.15] Alteración de la información	P		1			
[E.19] Fugas de información	P			1		
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	P	1				
[E.24] Caída del sistema por agotamiento de los recursos	MA	5				
[E.25] Pérdida de equipos	P	2		5		
[E.28] Indisponibilidad del personal	P	1				
[A.7] Uso no previsto	MA	1		1		
[A.11] Acceso no autorizado	MA	1	1	5		
[A.15] Modificación de la información	MA		5			
[A.18] Destrucción de la información	MA	1				
[A.19] Revelación de información	CS			2		
[A.23] Manipulación del hardware	P	10		5		
[A.24] Denegación de servicio	MA	10				
[A.25] Robo de equipos	P	2		5		
[A.26] Ataque destructivo	MA	10				
[A.28] Indisponibilidad del personal	P	5				
[A.29] Extorsión	MA	1	2	2		
[A.30] Ingeniería social (picaresca)	P	1	2	2		
Total		10	5	5	10	10
[N.1] Fuego	PP	10				
[N.2] Daños por agua	PP	5				
[N.*] Desastres naturales	PP	10				
[I.1] Fuego	P	10				
[I.2] Daños por agua	P	5				
[I.*] Desastres industriales	P	10				
[I.3] Contaminación medioambiental	PP	5				
[I.4] Contaminación electromagnética	P	1				
[I.5] Avería de origen físico o lógico	P	5				
[HW-CT] [I.6] Corte del suministro eléctrico	P	10				
CENTRAL [I.7] Condiciones inadecuadas de temperatura o humedad	P	10				
IP [E.1] Errores de los usuarios	P	1	1	1		
[E.2] Errores del administrador del sistema / de la seguridad	P	2	2	2		
[E.15] Alteración de la información	P		1			
[E.18] Destrucción de la información	P	1				
[E.19] Fugas de información	P			1		
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	P	1				
[E.24] Caída del sistema por agotamiento de los recursos	MA	5				
[E.25] Pérdida de equipos	P	10		5		
[E.28] Indisponibilidad del personal	P	1				
[A.5] Suplantación de la identidad	MA		5	5	10	
[A.6] Abuso de privilegios de acceso	MA	0	1	1	10	

	[A.7] Uso no previsto	MA	0	1	1		
	[A.11] Acceso no autorizado	MA	1	1	5	10	
	[A.13] Repudio (negación de actuaciones)	MA					10
	[A.15] Modificación de la información	CS		5			
	[A.18] Destrucción de la información	MA	5				
	[A.19] Revelación de información	CS			2		
	[A.23] Manipulación del hardware	P	5		5		
	[A.24] Denegación de servicio	CS	10				
	[A.25] Robo de equipos	P	10		5		
	[A.26] Ataque destructivo	MA	10				
	[A.28] Indisponibilidad del personal	P	5				
	[A.29] Extorsión	MA	1	2	2		
	[A.30] Ingeniería social (picaresca)	P	1	2	2		
	Total		10	5	5	10	10
	[N.1] Fuego	PP	10				
	[N.2] Daños por agua	PP	5				
	[N.*] Desastres naturales	PP	10				
	[I.1] Fuego	P	10				
	[I.2] Daños por agua	P	5				
	[I.*] Desastres industriales	P	10				
	[I.3] Contaminación medioambiental	PP	5				
	[I.4] Contaminación electromagnética	P	1				
	[I.5] Avería de origen físico o lógico	P	5				
	[I.6] Corte del suministro eléctrico	P	10				
	[I.7] Condiciones inadecuadas de temperatura o humedad	P	10				
	[E.1] Errores de los usuarios	P	1	1	1		
	[E.2] Errores del administrador del sistema / de la seguridad	P	2	2	2		
[HW-TM] TELEFONIA MOVIL	[E.15] Alteración de la información	P		1			
	[E.18] Destrucción de la información	P	1				
	[E.19] Fugas de información	P			1		
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	P	1				
	[E.24] Caída del sistema por agotamiento de los recursos	MA	5				
	[E.25] Pérdida de equipos	MA	0		1		
	[E.28] Indisponibilidad del personal	P	1				
	[A.5] Suplantación de la identidad	MA		5	5	10	
	[A.6] Abuso de privilegios de acceso	MA	0	1	1	10	
	[A.7] Uso no previsto	MA	0	1	1		
	[A.11] Acceso no autorizado	MA	1	1	5	10	
	[A.15] Modificación de la información	CS		5			
	[A.18] Destrucción de la información	MA	5				
	[A.19] Revelación de información	CS			2		
	[A.23] Manipulación del hardware	P	5		5		
	[A.24] Denegación de servicio	CS	10				

	[A.25] Robo de equipos	CS	0	1		
	[A.26] Ataque destructivo	MA	10			
	[A.28] Indisponibilidad del personal	P	5			
	[A.29] Extorsión	MA	1	2	2	
	[A.30] Ingeniería social (picaresca)	MA	1	2	2	
	Total		10	5	5	
	[N.1] Fuego	PP	10			
	[N.2] Daños por agua	PP	5			
	[N.*] Desastres naturales	PP	10			
	[I.1] Fuego	P	10			
	[I.2] Daños por agua	P	5			
	[I.*] Desastres industriales	P	10			
	[I.3] Contaminación medioambiental	PP	5			
	[I.4] Contaminación electromagnética	P	1			
	[I.5] Avería de origen físico o lógico	P	5			
	[I.6] Corte del suministro eléctrico	P	10			
	[I.7] Condiciones inadecuadas de temperatura o humedad	P	10			
	[E.15] Alteración de la información	P		1		
	[E.19] Fugas de información	P			1	
[HW-FIRE] FIREWALL	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	P	1			
	[E.24] Caída del sistema por agotamiento de los recursos	MA	5			
	[E.25] Pérdida de equipos	P	2		5	
	[E.28] Indisponibilidad del personal	P	1			
	[A.7] Uso no previsto	MA	1		1	
	[A.11] Acceso no autorizado	MA	1	1	5	
	[A.15] Modificación de la información	MA		5		
	[A.18] Destrucción de la información	MA	1			
	[A.19] Revelación de información	CS			2	
	[A.23] Manipulación del hardware	P	10		5	
	[A.24] Denegación de servicio	MA	10			
	[A.25] Robo de equipos	P	2		5	
	[A.26] Ataque destructivo	MA	10			
	[A.28] Indisponibilidad del personal	P	5			
	[A.29] Extorsión	MA	1	2	2	
	[A.30] Ingeniería social (picaresca)	P	1	2	2	
	Total		5	5	5	10
	[I.8] Fallo de servicios de comunicaciones	P	5			
	[E.2] Errores del administrador del sistema / de la seguridad	P	2	2	2	
[COM-LAN] RED LAN	[E.9] Errores de [re-]encaminamiento	P			1	
	[E.10] Errores de secuencia	P		1		
	[E.15] Alteración de la información	P		1		
	[E.19] Fugas de información	P			1	
	[E.24] Caída del sistema por agotamiento de los recursos	P	5			

	[E.28] Indisponibilidad del personal	P	1					
	[A.5] Suplantación de la identidad	MA		1	5	10		
	[A.7] Uso no previsto	MA	1	1	1			
	[A.9] [Re-]encaminamiento de mensajes	MA			1			
	[A.10] Alteración de secuencia	MA		1				
	[A.11] Acceso no autorizado	MA		1	5	10		
	[A.15] Modificación de la información	MA		5				
	[A.18] Destrucción de la información	MA	5					
	[A.19] Revelación de información	CS			2			
	[A.24] Denegación de servicio	CS	5					
	[A.28] Indisponibilidad del personal	P	5					
	[A.29] Extorsión	MA	1	2	2			
	[A.30] Ingeniería social (picaresca)	P	1	2	2			
	Total			10	10	10	10	10
	[I.8] Fallo de servicios de comunicaciones	P	10					
	[E.2] Errores del administrador del sistema / de la seguridad	P	2	2	2			
	[E.9] Errores de [re-]encaminamiento	P			1			
	[E.10] Errores de secuencia	P		1				
	[E.15] Alteración de la información	P		1				
	[E.18] Destrucción de la información	P	1					
	[E.19] Fugas de información	P			1			
	[E.24] Caída del sistema por agotamiento de los recursos	P	5					
	[E.28] Indisponibilidad del personal	P	1					
[COM-FO]	[A.5] Suplantación de la identidad	MA		10	10	10		
FIBRA	[A.7] Uso no previsto	MA	1	1	1			
OPTICA	[A.9] [Re-]encaminamiento de mensajes	MA			1			
	[A.10] Alteración de secuencia	MA		1				
	[A.11] Acceso no autorizado	MA		1	5	10		
	[A.13] Repudio (negación de actuaciones)	MA						10
	[A.14] Interceptación de información (escucha)	MA			1			
	[A.15] Modificación de la información	MA		5				
	[A.18] Destrucción de la información	MA	5					
	[A.19] Revelación de información	CS			5			
	[A.24] Denegación de servicio	CS	5					
	[A.28] Indisponibilidad del personal	P	5					
	[A.29] Extorsión	MA	1	2	2			
	[A.30] Ingeniería social (picaresca)	P	1	2	2			
	Total			10	10	10	10	10
	[I.8] Fallo de servicios de comunicaciones	P	10					
[COM-VPN]	[E.2] Errores del administrador del sistema / de la seguridad	P	2	2	2			
CONEXIÓN	[E.9] Errores de [re-]encaminamiento	P			1			
VPN	[E.10] Errores de secuencia	P		1				
	[E.15] Alteración de la información	P		1				
	[E.18] Destrucción de la información	P	1					

	[E.19] Fugas de información	P		1		
	[E.24] Caída del sistema por agotamiento de los recursos	P	5			
	[E.28] Indisponibilidad del personal	P	1			
	[A.5] Suplantación de la identidad	MA		10	10	10
	[A.7] Uso no previsto	MA	1	1	1	
	[A.9] [Re-]encaminamiento de mensajes	MA			1	
	[A.10] Alteración de secuencia	MA		1		
	[A.11] Acceso no autorizado	MA		1	5	10
	[A.13] Repudio (negación de actuaciones)	MA				10
	[A.14] Interceptación de información (escucha)	MA			1	
	[A.15] Modificación de la información	MA		5		
	[A.18] Destrucción de la información	MA	5			
	[A.19] Revelación de información	CS			5	
	[A.24] Denegación de servicio	CS	5			
	[A.28] Indisponibilidad del personal	P	5			
	[A.29] Extorsión	MA	1	2	2	
	[A.30] Ingeniería social (picaresca)	P	1	2	2	
	Total		5			10
	[I.8] Fallo de servicios de comunicaciones	P	5			
	[E.2] Errores del administrador del sistema / de la seguridad	P	2			
	[E.24] Caída del sistema por agotamiento de los recursos	P	5			
	[E.28] Indisponibilidad del personal	P	1			
[COM-WIFI] RED INALAMBRI CA	[A.5] Suplantación de la identidad	MA				10
	[A.7] Uso no previsto	MA	1			
	[A.11] Acceso no autorizado	MA				10
	[A.18] Destrucción de la información	MA	5			
	[A.24] Denegación de servicio	CS	5			
	[A.28] Indisponibilidad del personal	P	5			
	[A.29] Extorsión	MA	1			
	[A.30] Ingeniería social (picaresca)	P	1			
	Total		10			
	[N.1] Fuego	PP	10			
	[N.2] Daños por agua	PP	5			
	[N.*] Desastres naturales	PP	10			
	[I.1] Fuego	P	10			
[AUX-FA] FUENTES DE ALIMENTA CION	[I.2] Daños por agua	P	5			
	[I.*] Desastres industriales	P	10			
	[I.3] Contaminación medioambiental	PP	5			
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	P	1			
	[E.28] Indisponibilidad del personal	P	1			
	[A.7] Uso no previsto	MA	5			
	[A.18] Destrucción de la información	MA	1			
	[A.23] Manipulación del hardware	MA	5			

	[A.25] Robo de equipos	P	10		
	[A.26] Ataque destructivo	MA	10		
	[A.28] Indisponibilidad del personal	P	5		
	[A.29] Extorsión	MA	1		
	[A.30] Ingeniería social (picaresca)	P	1		
	Total		10	10	10
	[N.1] Fuego	PP	10		
	[N.2] Daños por agua	PP	5		
	[N.*] Desastres naturales	PP	10		
	[I.1] Fuego	P	10		
	[I.2] Daños por agua	P	5		
	[I.*] Desastres industriales	P	10		
	[I.3] Contaminación medioambiental	PP	5		
	[E.15] Alteración de la información	P		1	
	[E.19] Fugas de información	P			1
[AUX- CCTV] SISTEMA DE CCTV	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	P	1		
	[A.7] Uso no previsto	MA	5	0	0
	[A.15] Modificación de la información	MA		5	
	[A.18] Destrucción de la información	MA	1		
	[A.19] Revelación de información	CS			5
	[A.23] Manipulación del hardware	MA	5		5
	[A.25] Robo de equipos	P	1		
	[A.26] Ataque destructivo	MA	1		
	[A.28] Indisponibilidad del personal	P	2		
	[A.29] Extorsión	MA	5	10	10
	[A.30] Ingeniería social (picaresca)	P	5	10	10
	Total		5		
	[N.1] Fuego	PP	1		
	[N.2] Daños por agua	PP	1		
	[N.*] Desastres naturales	PP	1		
	[I.1] Fuego	P	1		
	[I.2] Daños por agua	P	1		
	[I.*] Desastres industriales	P	1		
[AUX-AA] AIRE ACONDICI ONADO	[I.3] Contaminación medioambiental	PP	1		
	[I.6] Corte del suministro eléctrico	P	1		
	[I.9] Interrupción de otros servicios o suministros esenciales	P	1		
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	P	1		
	[E.28] Indisponibilidad del personal	P	1		
	[A.7] Uso no previsto	MA	1		
	[A.18] Destrucción de la información	MA	1		
	[A.23] Manipulación del hardware	MA	1		
	[A.25] Robo de equipos	P	1		
	[A.26] Ataque destructivo	MA	1		

	[A.28] Indisponibilidad del personal	P	2			
	[A.29] Extorsión	MA	5			
	[A.30] Ingeniería social (picaresca)	P	5			
	Total		5			
	[E.28] Indisponibilidad del personal	P	1			
[AUX-UPS] UPS	[A.18] Destrucción de la información	MA	1			
	[A.28] Indisponibilidad del personal	P	5			
	[A.29] Extorsión	MA	1			
	[A.30] Ingeniería social (picaresca)	P	1			
	Total		5			
	[E.28] Indisponibilidad del personal	P	1			
[AUX-GE] GRUPO ELECTROG ENO	[A.18] Destrucción de la información	MA	1			
	[A.28] Indisponibilidad del personal	P	5			
	[A.29] Extorsión	MA	1			
	[A.30] Ingeniería social (picaresca)	P	1			
	Total		10			
	[N.1] Fuego	PP	10			
	[N.2] Daños por agua	PP	5			
	[N.*] Desastres naturales	PP	10			
	[I.1] Fuego	P	10			
	[I.2] Daños por agua	P	5			
	[I.*] Desastres industriales	P	10			
	[I.3] Contaminación medioambiental	PP	5			
	[I.4] Contaminación electromagnética	P	1			
[AUX-CD] CABLEADO DE DATOS	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	P	1			
	[E.28] Indisponibilidad del personal	P	1			
	[A.7] Uso no previsto	MA	5			
	[A.18] Destrucción de la información	MA	1			
	[A.23] Manipulación del hardware	MA	5			
	[A.25] Robo de equipos	MA	10			
	[A.26] Ataque destructivo	MA	10			
	[A.28] Indisponibilidad del personal	P	5			
	[A.29] Extorsión	MA	1			
	[A.30] Ingeniería social (picaresca)	P	1			
	Total		10	10	10	
	[N.1] Fuego	P	10			
	[N.2] Daños por agua	P	10			
	[N.*] Desastres naturales	P	10			
[L-ARQ] DATA CENTER OFICINA AREQUIPA	[I.1] Fuego	P	10			
	[I.2] Daños por agua	P	10			
	[I.*] Desastres industriales	P	10			
	[I.3] Contaminación medioambiental	P	1			
	[I.4] Contaminación electromagnética	PP	1			

	[E.15] Alteración de la información	P	1			
	[E.19] Fugas de información	P		1		
	[E.28] Indisponibilidad del personal	P	1			
	[A.6] Abuso de privilegios de acceso	MA	1			
	[A.7] Uso no previsto	MA	1			
	[A.15] Modificación de la información	MA		5		
	[A.18] Destrucción de la información	MA	1			
	[A.19] Revelación de información	CS			5	
	[A.26] Ataque destructivo	P	10			
	[A.27] Ocupación enemiga	MA	10			
	[A.28] Indisponibilidad del personal	P	2			
	[A.29] Extorsión	MA	5	10	10	
	[A.30] Ingeniería social (picaresca)	P	5	10	10	
	Total		10	10	10	
	[N.1] Fuego	P	10			
	[N.2] Daños por agua	P	10			
	[N.*] Desastres naturales	P	10			
	[I.1] Fuego	P	10			
	[I.2] Daños por agua	P	10			
	[I.*] Desastres industriales	P	10			
	[I.3] Contaminación medioambiental	P	1			
	[I.4] Contaminación electromagnética	PP	1			
[L-SC] DATA CENTER OFICINA SANTA CRUZ	[E.15] Alteración de la información	P		1		
	[E.19] Fugas de información	P			1	
	[E.28] Indisponibilidad del personal	P	1			
	[A.6] Abuso de privilegios de acceso	MA	1			
	[A.7] Uso no previsto	MA	1			
	[A.15] Modificación de la información	MA		5		
	[A.18] Destrucción de la información	MA	1			
	[A.19] Revelación de información	CS			5	
	[A.26] Ataque destructivo	P	10			
	[A.27] Ocupación enemiga	MA	10			
	[A.28] Indisponibilidad del personal	P	2			
	[A.29] Extorsión	MA	5	10	10	
	[A.30] Ingeniería social (picaresca)	P	5	10	10	
	Total		5	10	10	10
	[E.15] Alteración de la información	P		1		
	[E.19] Fugas de información	P			1	
[P-AIT] PERSONAL ADMINISTRACION IT	[E.28] Indisponibilidad del personal	P	1			
	[A.5] Suplantación de la identidad	CS		1	5	10
	[A.6] Abuso de privilegios de acceso	CS	0	1	5	
	[A.11] Acceso no autorizado	CS		1	5	
	[A.15] Modificación de la información	MA		5		
	[A.18] Destrucción de la información	MA	1			

	[A.19] Revelación de información	CS		5		
	[A.28] Indisponibilidad del personal	P	2			
	[A.29] Extorsión	MA	5	10	10	
	[A.30] Ingeniería social (picaresca)	P	5	10	10	
	Total		5	10	10	10
	[E.15] Alteración de la información	P		1		
	[E.19] Fugas de información	P			1	
	[E.28] Indisponibilidad del personal	P	2			
	[A.5] Suplantación de la identidad	CS		1	5	10
[P-DIT]	[A.6] Abuso de privilegios de acceso	CS	0	1	5	
PERSONAL	[A.11] Acceso no autorizado	CS		1	5	
DESARROL	[A.15] Modificación de la información	MA		5		
LO IT	[A.18] Destrucción de la información	MA	1			
	[A.19] Revelación de información	CS			5	
	[A.28] Indisponibilidad del personal	P	2			
	[A.29] Extorsión	MA	5	10	10	
	[A.30] Ingeniería social (picaresca)	P	5	10	10	

Nota: Elaboración propia.

ANEXO N° 10 IDENTIFICACIÓN Y VALORACION DE SALVAGUARDAS

Tabla 70.

Identificación y valoración de las salvaguardas

ASPECTO	TPD	RECOMEN	SEM	SALVAGUARDA	CURRENT	TARGET	PILAR
G	EL	8		[IA] Identificación y autenticación	L0-L2	L3-L4	L2-L5
T	EL	7		[AC] Control de acceso lógico	L1	L4	L2-L4
G	PR	8		[D] Protección de la Información	L1	L4	L2-L5
G	EL			[K] Protección de claves criptográficas			n.a.
G	PR	6		[S] Protección de los Servicios	L1	L4	L2-L4
G	PR	7		[SW] Protección de las Aplicaciones Informáticas (SW)	L1	L4	L2-L4
G	PR	7		[HW] Protección de los Equipos Informáticos (HW)	L1	L4	L2-L4
G	PR	8		[COM] Protección de las Comunicaciones	L1	L4	L2-L5
G	PR			[IP] Sistema de protección de frontera lógica			n.a.
G	PR	7		[MP] Protección de los Soportes de Información	L1	L1	L2-L4
G	PR	6		[AUX] Elementos Auxiliares	L1	L4	L2-L4
F	EL	6		[PPE] Protección física de los equipos	L2	L4	L3-L4
F	PR	7		[L] Protección de las Instalaciones	L2	L4	L2-L4
F	EL			[PPS] Protección del perímetro físico			n.a.
P	PR	6		[PS] Gestión del Personal	L1	L4	L2-L4
G	PR			[PDS] Servicios potencialmente peligrosos			n.a.
G	CR	6		[IR] Gestión de incidentes	L0	L4	L2-L4
T	PR	8		[tools] Herramientas de seguridad	L2	L4	L3-L5
G	CR	6		[V] Gestión de vulnerabilidades	L0	L4	L2-L4
T	MN			[A] Registro y auditoría			n.a.
G	RC	5		[BC] Continuidad del negocio	L1	L3	L2-L3
G	AD	5		[G] Organización	L1	L3	L2-L3
G	AD	6		[E] Relaciones Externas	L0	L3	L3-L4
G	AD	5		[NEW] Adquisición / desarrollo	L1	L3	L2-L3

Nota: Elaboración propia.

ANEXO N° 11 RIESGO POTENCIAL DE LOS ACTIVOS

Tabla 71.

Riesgo potencial de los activos

activo	[D]	[I]	[C]	[A]	[T]
ACTIVOS	{6,7}	{6,7}	{7,0}	{7,6}	{5,7}
[S] SERVICIOS	{6,1}	{5,6}	{7,0}	{7,6}	{5,7}
[SG-SISGECO] SISTEMA DE GESTIÓN SISGECO	{6,1}	{5,6}	{7,0}	{7,6}	{5,7}
[E] EQUIPAMIENTO	{6,7}	{6,7}	{7,0}	{7,6}	{5,7}
[SW] APLICACIONES	{6,7}	{6,7}	{7,0}	{7,6}	{5,7}
[SW-SSP] SOFTWARE STAR SOFT PLANILLAS	{6,1}	{6,2}	{7,0}	{7,6}	{5,7}
[SW-SISCONT] SOFTWARE SISCONT	{6,1}	{6,2}	{7,0}	{7,6}	{5,7}
[SW-GBD] SISTEMA DE GESTION DE BASE DE DATOS	{6,1}	{6,2}	{6,2}	{5,8}	{5,7}
[SW-INTRANET] SISTEMA INTRANET	{4,4}	{4,4}	{4,4}	{4,0}	{3,9}
[SW-ANTIVIRUS] ANTIVIRUS BITDEFENDER	{5,8}	{5,8}	{6,2}		
[SW-SO] SISTEMA OPERATIVO	{6,1}	{6,2}	{6,2}	{5,8}	{5,7}
[SW-OF] OFIMATICA	{4,0}	{5,8}	{6,2}		
[BCK] BACKUPS	{6,7}	{6,7}	{7,0}	{7,6}	{5,7}
[SW-CC] CORREO CORPORATIVO	{5,8}	{6,7}	{7,0}	{6,7}	{5,0}
[HW] EQUIPOS	{6,7}	{6,2}	{7,0}	{7,6}	{5,7}
[HW-SBD] SERVIDOR DE BASE DE DATOS	{6,0}	{5,8}	{7,0}	{6,7}	
[HW-PC] COMPUTADORA DE ESCRITORIO	{6,7}	{6,2}	{7,0}	{7,6}	{5,7}
[HW-IMP] IMPRESORAS	{4,9}		{5,3}	{5,8}	
[HW-AP] SERVIDOR APLICACIONES	{6,0}	{5,8}	{7,0}	{6,7}	
[HW-SW] SWITCH	{6,0}	{5,3}	{5,5}		
[HW-CT] CENTRAL IP	{6,7}	{6,2}	{5,5}	{5,8}	{5,7}
[HW-TM] TELEFONIA MOVIL	{5,5}	{5,0}	{3,7}	{4,6}	
[HW-FIRE] FIREWALL	{6,0}	{5,3}	{5,5}		
[COM] COMUNICACIONES	{6,1}	{5,8}	{6,2}	{5,8}	{5,0}
[COM-LAN] RED LAN	{6,1}	{5,3}	{5,5}	{5,8}	
[COM-FO] FIBRA OPTICA	{6,1}	{5,8}	{6,2}	{5,8}	{5,0}
[COM-VPN] CONEXIÓN VPN	{6,1}	{5,8}	{6,2}	{5,8}	{5,0}

[COM-WIFI] RED INALAMBRICA	{4,4}			{5,2}
[AUX] ELEMENTOS AUXILIARES	{5,2}	{5,6}	{6,2}	
[AUX-FA] FUENTES DE ALIMENTACION	{3,3}			
[AUX-CCTV] SISTEMA DE CCTV	{5,2}	{5,6}	{6,2}	
[AUX-AA] AIRE ACONDICIONADO	{3,9}			
[AUX-UPS] UPS	{4,2}			
[AUX-GE] GRUPO ELECTROGENO	{3,6}			
[AUX-CD] CABLEADO DE DATOS	{4,5}			
[L] INSTALACIONES	{5,6}	{5,6}	{6,2}	
[L-ARQ] DATA CENTER OFICINA AREQUIPA	{5,6}	{5,6}	{6,2}	
[L-SC] DATA CENTER OFICINA SANTA CRUZ	{5,6}	{5,6}	{6,2}	
[P] PERSONAL	{5,1}	{5,8}	{7,0}	{6,7}
[P-AIT] PERSONAL ADMINISTRACION IT	{5,1}	{5,8}	{7,0}	{6,7}
[P-DIT] PERSONAL DESARROLLO IT	{3,9}	{3,5}	{5,9}	{4,3}

Nota: Elaboración propia.

ANEXO N° 12 RIESGO RESIDUAL DE LOS ACTIVOS

Tabla 72.

Riesgo residual de los activos

activo	[D]	[I]	[C]	[A]	[T]
ACTIVOS	{2,7}	{2,7}	{3,2}	{3,5}	{1,8}
[S] SERVICIOS	{1,9}	{1,3}	{2,7}	{3,3}	{1,6}
[SG-SISGECO] SISTEMA DE GESTIÓN SISGECO	{1,9}	{1,3}	{2,7}	{3,3}	{1,6}
[E] EQUIPAMIENTO	{2,7}	{2,7}	{3,0}	{3,5}	{1,8}
[SW] APLICACIONES	{2,7}	{2,7}	{3,0}	{3,5}	{1,8}
[SW-SSP] SOFTWARE STAR SOFT PLANILLAS	{1,9}	{1,9}	{2,7}	{3,3}	{1,6}
[SW-SISCONT] SOFTWARE SISCONT	{1,9}	{1,9}	{2,7}	{3,3}	{1,6}
[SW-GBD] SISTEMA DE GESTION DE BASE DE DATOS	{1,9}	{1,8}	{1,8}	{1,7}	{1,5}
[SW-INTRANET] SISTEMA INTRANET	{0,82}	{0,81}	{0,81}	{0,78}	{0,74}
[SW-ANTIVIRUS] ANTIVIRUS BITDEFENDER	{1,5}	{1,5}	{1,8}		
[SW-SO] SISTEMA OPERATIVO	{1,9}	{1,8}	{1,8}	{1,7}	{1,5}
[SW-OF] OFIMATICA	{0,74}	{1,5}	{1,8}		
[BCK] BACKUPS	{2,7}	{2,7}	{3,0}	{3,5}	{1,8}
[SW-CC] CORREO CORPORATIVO	{1,6}	{2,4}	{2,8}	{2,5}	{0,98}
[HW] EQUIPOS	{2,7}	{2,2}	{3,0}	{3,5}	{1,8}
[HW-SBD] SERVIDOR DE BASE DE DATOS	{2,0}	{1,8}	{3,0}	{2,7}	
[HW-PC] COMPUTADORA DE ESCRITORIO	{2,7}	{2,2}	{3,0}	{3,5}	{1,8}
[HW-IMP] IMPRESORAS	{0,98}		{1,2}	{1,7}	
[HW-AP] SERVIDOR APLICACIONES	{2,0}	{1,8}	{3,0}	{2,7}	
[HW-SW] SWITCH	{2,0}	{1,2}	{1,4}		
[HW-CT] CENTRAL IP	{2,7}	{2,1}	{1,4}	{1,8}	{1,7}
[HW-TM] TELEFONIA MOVIL	{1,5}	{0,98}	{0,72}	{0,92}	
[HW-FIRE] FIREWALL	{2,0}	{1,2}	{1,4}		
[COM] COMUNICACIONES	{2,3}	{2,0}	{2,3}	{2,1}	{1,1}
[COM-LAN] RED LAN	{2,3}	{1,3}	{1,5}	{2,0}	
[COM-FO] FIBRA OPTICA	{2,3}	{2,0}	{2,3}	{2,1}	{1,1}
[COM-VPN] CONEXIÓN VPN	{2,3}	{2,0}	{2,3}	{2,1}	{1,1}
[COM-WIFI] RED INALAMBRICA	{0,89}			{1,4}	
[AUX] ELEMENTOS AUXILIARES	{1,4}	{1,7}	{2,3}		

[AUX-FA] FUENTES DE ALIMENTACION	{0,70}			
[AUX-CCTV] SISTEMA DE CCTV	{1,4}	{1,7}	{2,3}	
[AUX-AA] AIRE ACONDICIONADO	{0,80}			
[AUX-UPS] UPS	{0,86}			
[AUX-GE] GRUPO ELECTROGENO	{0,74}			
[AUX-CD] CABLEADO DE DATOS	{0,94}			
[L] INSTALACIONES	{1,9}	{1,8}	{2,3}	
[L-ARQ] DATA CENTER OFICINA AREQUIPA	{1,9}	{1,8}	{2,3}	
[L-SC] DATA CENTER OFICINA SANTA CRUZ	{1,9}	{1,8}	{2,3}	
[P] PERSONAL	{1,2}	{1,9}	{3,2}	{2,8}
[P-AIT] PERSONAL ADMINISTRACION IT	{1,2}	{1,9}	{3,2}	{2,8}
[P-DIT] PERSONAL DESARROLLO IT	{0,81}	{0,72}	{2,0}	{0,88}

Nota: Elaboración propia.

**ANEXO N° 13 IMPACTO POTENCIAL SOBRE CADA UNO DE LOS
ACTIVOS**

Tabla 73.

Impacto potencial sobre cada uno de los activos

activo	[D]	[I]	[C]	[A]	[T]
ACTIVOS	[7]	[7]	[7]	[7]	[6]
[S] SERVICIOS	[7]	[6]	[7]	[7]	[6]
[SG-SISGECO] SISTEMA DE GESTIÓN SISGECO	[7]	[6]	[7]	[7]	[6]
[E] EQUIPAMIENTO	[7]	[7]	[7]	[7]	[6]
[SW] APLICACIONES	[7]	[7]	[7]	[7]	[6]
[SW-SSP] SOFTWARE STAR SOFT PLANILLAS	[7]	[7]	[7]	[7]	[6]
[SW-SISCONT] SOFTWARE SISCONT	[7]	[7]	[7]	[7]	[6]
[SW-GBD] SISTEMA DE GESTION DE BASE DE DATOS	[7]	[7]	[7]	[7]	[6]
[SW-INTRANET] SISTEMA INTRANET	[4]	[4]	[4]	[4]	[3]
[SW-ANTIVIRUS] ANTIVIRUS BITDEFENDER	[7]	[7]	[7]		
[SW-SO] SISTEMA OPERATIVO	[7]	[7]	[7]	[7]	[6]
[SW-OF] OFIMATICA	[4]	[7]	[7]	[7]	
[BCK] BACKUPS	[7]	[7]	[7]	[7]	[6]
[SW-CC] CORREO CORPORATIVO	[7]	[7]	[7]	[7]	[6]
[HW] EQUIPOS	[7]	[7]	[7]	[7]	[6]
[HW-SBD] SERVIDOR DE BASE DE DATOS	[7]	[7]	[7]	[7]	
[HW-PC] COMPUTADORA DE ESCRITORIO	[7]	[7]	[7]	[7]	[6]
[HW-IMP] IMPRESORAS	[4]		[3]	[4]	
[HW-AP] SERVIDOR APLICACIONES	[7]	[7]	[7]	[7]	
[HW-SW] SWITCH	[7]	[6]	[6]		
[HW-CT] CENTRAL IP	[7]	[6]	[6]	[7]	[6]
[HW-TM] TELEFONIA MOVIL	[5]	[4]	[3]	[5]	
[HW-FIRE] FIREWALL	[7]	[6]	[6]		
[COM] COMUNICACIONES	[7]	[7]	[7]	[7]	[6]
[COM-LAN] RED LAN	[6]	[6]	[6]	[7]	
[COM-FO] FIBRA OPTICA	[7]	[7]	[7]	[7]	[6]
[COM-VPN] CONEXIÓN VPN	[7]	[7]	[7]	[7]	[6]
[COM-WIFI] RED INALAMBRICA	[3]			[6]	
[AUX] ELEMENTOS AUXILIARES	[7]	[7]	[7]		
[AUX-FA] FUENTES DE ALIMENTACION	[3]				
[AUX-CCTV] SISTEMA DE CCTV	[7]	[7]	[7]		
[AUX-AA] AIRE ACONDICIONADO	[4]				
[AUX-UPS] UPS	[5]				
[AUX-GE] GRUPO ELECTROGENO	[4]				
[AUX-CD] CABLEADO DE DATOS	[5]				
[L] INSTALACIONES	[7]	[7]	[7]		
[L-ARQ] DATA CENTER OFICINA AREQUIPA	[7]	[7]	[7]		

[L-SC] DATA CENTER OFICINA SANTA CRUZ	[7]	[7]	[7]	
[P] PERSONAL	[6]	[7]	[7]	[7]
[P-AIT] PERSONAL ADMINISTRACION IT	[6]	[7]	[7]	[7]
[P-DIT] PERSONAL DESARROLLO IT	[4]	[3]	[5]	[3]

Nota: Elaboración propia.

ANEXO N° 14 IMPACTO RESIDUAL

Tabla 74.

Impacto residual acumulado

activo	[D]	[I]	[C]	[A]	[T]
ACTIVOS	[6]	[6]	[6]	[6]	[5]
[S] SERVICIOS	[6]	[5]	[6]	[6]	[5]
[SG-SISGECO] SISTEMA DE GESTIÓN SISGECO	[6]	[5]	[6]	[6]	[5]
[E] EQUIPAMIENTO	[6]	[6]	[6]	[6]	[5]
[SW] APLICACIONES	[6]	[6]	[6]	[6]	[5]
[SW-SSP] SOFTWARE STAR SOFT PLANILLAS	[6]	[6]	[6]	[6]	[5]
[SW-SISCONT] SOFTWARE SISCONT	[6]	[6]	[6]	[6]	[5]
[SW-GBD] SISTEMA DE GESTION DE BASE DE DATOS	[5]	[5]	[5]	[6]	[4]
[SW-INTRANET] SISTEMA INTRANET	[2]	[2]	[2]	[3]	[1]
[SW-ANTIVIRUS] ANTIVIRUS BITDEFENDER	[5]	[5]	[5]		
[SW-SO] SISTEMA OPERATIVO	[5]	[5]	[5]	[6]	[4]
[SW-OF] OFIMATICA	[2]	[5]	[5]		
[BCK] BACKUPS	[6]	[6]	[6]	[6]	[5]
[SW-CC] CORREO CORPORATIVO	[6]	[6]	[6]	[6]	[5]
[HW] EQUIPOS	[6]	[6]	[6]	[6]	[5]
[HW-SBD] SERVIDOR DE BASE DE DATOS	[6]	[6]	[6]	[6]	
[HW-PC] COMPUTADORA DE ESCRITORIO	[6]	[6]	[6]	[6]	[5]
[HW-IMP] IMPRESORAS	[3]		[2]	[3]	
[HW-AP] SERVIDOR APLICACIONES	[6]	[6]	[6]	[6]	
[HW-SW] SWITCH	[6]	[5]	[5]		
[HW-CT] CENTRAL IP	[6]	[5]	[5]	[6]	[5]
[HW-TM] TELEFONIA MOVIL	[4]	[3]	[2]	[4]	
[HW-FIRE] FIREWALL	[6]	[5]	[5]		
[COM] COMUNICACIONES	[6]	[6]	[6]	[6]	[5]
[COM-LAN] RED LAN	[5]	[5]	[5]	[6]	
[COM-FO] FIBRA OPTICA	[6]	[6]	[6]	[6]	[5]
[COM-VPN] CONEXIÓN VPN	[6]	[6]	[6]	[6]	[5]
[COM-WIFI] RED INALAMBRICA	[2]			[5]	
[AUX] ELEMENTOS AUXILIARES	[6]	[5]	[5]		
[AUX-FA] FUENTES DE ALIMENTACION	[2]				
[AUX-CCTV] SISTEMA DE CCTV	[6]	[5]	[5]		
[AUX-AA] AIRE ACONDICIONADO	[3]				
[AUX-UPS] UPS	[4]				
[AUX-GE] GRUPO ELECTROGENO	[3]				
[AUX-CD] CABLEADO DE DATOS	[4]				
[L] INSTALACIONES	[5]	[5]	[5]		

[L-ARQ] DATA CENTER OFICINA AREQUIPA	[5]	[5]	[5]	
[L-SC] DATA CENTER OFICINA SANTA CRUZ	[5]	[5]	[5]	
[P] PERSONAL	[2]	[3]	[3]	[3]
[P-AIT] PERSONAL ADMINISTRACION IT	[5]	[6]	[6]	[6]
[P-DIT] PERSONAL DESARROLLO IT	[3]	[2]	[4]	[2]

Nota: Elaboración propia.

ANEXO N° 15 PERMISO PARA LA RECOLECCIÓN DE DATOS

MODELO DE AUTORIZACIÓN PARA EL RECOJO DE INFORMACIÓN

Lima, 02 de julio de 2020.

Quien suscribe: Sr.

Representante Legal – Empresa Deco Interiors S.A.C.

AUTORIZA: Permiso para recojo de información pertinente en función del proyecto de investigación, denominado:

INFLUENCIA DE LA METODOLOGÍA MAGERIT V3 EN LA SEGURIDAD DE INFORMACIÓN DE LA EMPRESA DECO INTERIORS S.A.C.

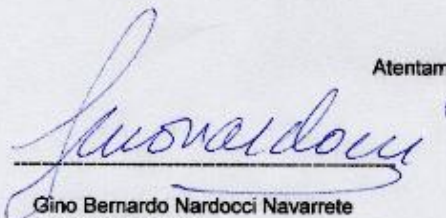
Por el presente, el que suscribe **Gino Bernardo Nardocci Navarrete**, representante legal de la empresa:

Deco Interiors S.A.C. AUTORIZO al alumno: **Ramiro Cabrejos Torres**, con DNI N° **44249996**, estudiante de la Escuela Profesional de Ingeniería de Sistemas, y autor del trabajo de investigación denominado:

INFLUENCIA DE LA METODOLOGÍA MAGERIT V3 EN LA SEGURIDAD DE INFORMACIÓN DE LA EMPRESA DECO INTERIORS S.A.C., al uso de dicha información que conforma el expediente técnico, así como hojas de memorias, cálculos entre otros como planos para efectos exclusivamente académicos de la elaboración de tesis para optar el título profesional de Ingeniero de Sistemas, enunciada líneas arriba. De quien solicita.

Se garantiza la absoluta confidencialidad de la información solicitada.

Atentamente.



Gino Bernardo Nardocci Navarrete
DNI N° 06372120
Gerente General

ANEXO N° 16 RESOLUCIÓN DE APROBACIÓN DE PROYECTO DE INVESTIGACIÓN

FACULTAD DE INGENIERÍA, ARQUITECTURA Y URBANISMO RESOLUCIÓN N° 2108-2020/FIAU-USS

Pimentel, 22 de septiembre de 2020

VISTO:

El Acta de reunión N°1409 - 2020, de fecha 14 de septiembre de 2020 del Comité de Investigación de la Escuela profesional de INGENIERÍA DE SISTEMAS, para la ejecución de la Tesis: "INCIDENCIA DE LA METODOLOGIA MAGERIT V3 EN LA SEGURIDAD DE INFORMACION DE LA EMPRESA DECO INTERIORS SAC.", presentado por CABREJOS TORRES RAMIRO, del Programa de estudios INGENIERÍA DE SISTEMAS, y;

CONSIDERANDO:

Que, de conformidad con la Ley Universitaria N° 30220 en su artículo 48º que a letra dice: "La investigación constituye una función esencial y obligatoria de la universidad, que la fomenta y realiza, respondiendo a través de la producción de conocimiento y desarrollo de tecnologías a las necesidades de la sociedad, con especial énfasis en la realidad nacional. Los docentes, estudiantes y graduados participan en la actividad investigadora en su propia institución o en redes de investigación nacional o internacional, creadas por las instituciones universitarias públicas o privadas.";

Que, de conformidad con el Reglamento de grados y títulos en su artículo 21º señala: "Los temas de trabajo de Investigación, trabajo académico y tesis son aprobados por el Comité de Investigación y derivados a la facultad o Escuela de Posgrado, según corresponda, para la emisión de la resolución respectiva. El período de vigencia de los mismos será de dos años, a partir de su aprobación. En caso un tema perdiera vigencia, el Comité de Investigación evaluará la ampliación de la misma.

Que, de conformidad con el Reglamento de grados y títulos en su artículo 24º señala: La tesis es un estudio que debe denotar rigurosidad metodológica, originalidad, relevancia social, utilidad teórica y/o práctica en el ámbito de la escuela profesional. Para el grado de doctor se requiere una tesis de máxima rigurosidad académica y de carácter original. Es individual para la obtención de un grado; es individual o en pares para obtener un título profesional. Asimismo, en su artículo 25º señala: "El tema debe responder a alguna de las líneas de investigación institucionales de la USS S.A.C."

Que, en el Acta de reunión N°1409 - 2020 de fecha 14 de septiembre de 2020, del Comité de Investigación de la Escuela profesional de INGENIERÍA DE SISTEMAS, se indica entre los acuerdos la aprobación del tema de la Tesis denominado "INCIDENCIA DE LA METODOLOGIA MAGERIT V3 EN LA SEGURIDAD DE INFORMACION DE LA EMPRESA DECO INTERIORS SAC." de la línea de investigación de INFRAESTRUCTURA, TECNOLOGÍA Y MEDIO AMBIENTE, a cargo de CABREJOS TORRES RAMIRO en condición de egresado, del Programa de estudios INGENIERÍA DE SISTEMAS.

Estando a lo expuesto, y en uso de las atribuciones conferidas y de conformidad con las normas y reglamentos vigentes;

SE RESUELVE:

ARTÍCULO 1º: APROBAR, el tema de la Tesis denominado "INCIDENCIA DE LA METODOLOGIA MAGERIT V3 EN LA SEGURIDAD DE INFORMACION DE LA EMPRESA DECO INTERIORS SAC.", perteneciente a la línea de investigación de INFRAESTRUCTURA, TECNOLOGÍA Y MEDIO AMBIENTE, a cargo de CABREJOS TORRES RAMIRO, del Programa de estudios INGENIERÍA DE SISTEMAS.

ARTÍCULO 2º: ESTABLECER, que la Inscripción del Título de la Tesis se realice a partir de emitida la presente resolución y tendrá una vigencia de dos (02) años.

ARTÍCULO 3º: DEJAR SIN EFECTO, toda Resolución emitida por la Facultad que se oponga a la presente Resolución.

REGÍSTRESE, COMUNÍQUESE Y ARCHÍVESE


 Dr. Mario Francisco Torres Miroso
Decano - Facultad de Ingeniería,
Arquitectura y Urbanismo
UNIVERSIDAD SEÑOR DE SIPÁN SAC.


 Dra. María Beatriz Salar Rivera
Decana Académica - Facultad de Ingeniería,
Arquitectura y Urbanismo
UNIVERSIDAD SEÑOR DE SIPÁN SAC.

Cc: interesado, Archivo

ANEXO N° 17 MODIFICACIÓN DE TÍTULO DE PROYECTO DE TESIS

FACULTAD DE INGENIERÍA, ARQUITECTURA Y URBANISMO RESOLUCIÓN N°2322-2020/FIAU-USS

Pimentel, 17 de noviembre de 2020

VISTOS:

El Acta de reunión N° 2610-2020 del Comité de investigación de la Escuela profesional de INGENIERÍA DE SISTEMAS remitida el 12 de noviembre de 2020 mediante oficio N° 0237-2020/FIAU-IS-USS de la Dirección de Escuela profesional de INGENIERÍA DE SISTEMAS, y;

CONSIDERANDO:

Que, de conformidad con la Ley Universitaria N° 30220 en su artículo 48° que a letra dice: "La investigación constituye una función esencial y obligatoria de la universidad, que la fomenta y realiza, respondiendo a través de la producción de conocimiento y desarrollo de tecnologías a las necesidades de la sociedad, con especial énfasis en la realidad nacional. Los docentes, estudiantes y graduados participan en la actividad investigadora en su propia institución o en redes de investigación nacional o internacional, creadas por las instituciones universitarias públicas o privadas.";

Que, de conformidad con el Reglamento de grados y títulos en su artículo 21° señala: "Los temas de trabajo de investigación, trabajo académico y tesis son aprobados por el Comité de Investigación y derivados a la facultad o Escuela de Posgrado, según corresponda, para la emisión de la resolución respectiva. El periodo de vigencia de los mismos será de dos años, a partir de su aprobación. En caso un tema perdiera vigencia, el Comité de Investigación evaluará la ampliación de la misma.

Que, de conformidad con el Reglamento de grados y títulos en su artículo 24° señala: La tesis es un estudio que debe denotar rigurosidad metodológica, originalidad, relevancia social, utilidad teórica y/o práctica en el ámbito de la escuela profesional. Para el grado de doctor se requiere una tesis de máxima rigurosidad académica y de carácter original. Es individual para la obtención de un grado; es individual o en pares para obtener un título profesional. Asimismo, en su artículo 25° señala: "El tema debe responder a alguna de las líneas de investigación institucionales de la USS S.A.C."

Que, según documentos de vistos el Comité de investigación de la Escuela profesional de INGENIERÍA DE SISTEMAS acuerda aprobar la modificación de los temas de Tesis a cargo de los estudiantes y/o egresados que se detallan en el anexo de la presente Resolución.

Estando a lo expuesto, y en uso de las atribuciones conferidas y de conformidad con las normas y reglamentos vigentes;

SE RESUELVE:

ARTÍCULO 1°: MODIFICAR, el tema de la Tesis perteneciente a la línea de investigación de INFRAESTRUCTURA, TECNOLOGÍA Y MEDIO AMBIENTE, a cargo de los estudiantes y/o egresados del Programa de estudios de **INGENIERÍA DE SISTEMAS** según se detalla en el anexo de la presente Resolución.

ARTÍCULO 2°: MODIFICAR, la Resolución de Facultad con la que se asigna Asesor especialista en el extremo del tema de la tesis quedando tal como se detalla en el anexo de la presente Resolución.

ARTÍCULO 3°: DEJAR SIN EFECTO, toda Resolución emitida por la Facultad que se oponga a la presente Resolución.

REGÍSTRESE, COMUNÍQUESE Y ARCHÍVESE



Dr. María Fernández Ramos Morad
Decano - Facultad de Ingeniería,
Arquitectura y Urbanismo
UNIVERSIDAD SEÑOR DE SIPÁN S.A.C.



MSc. María Rosalía Siles Rivera
Directora Académica / Escuela de Ingeniería,
Arquitectura y Urbanismo
UNIVERSIDAD SEÑOR DE SIPÁN S.A.C.

Cc: Interesado, Archivo

**FACULTAD DE INGENIERÍA, ARQUITECTURA Y URBANISMO
RESOLUCIÓN N°2322-2020/FIAU-USS**

Pimentel, 17 de noviembre de 2020

ANEXO

N°	APELLIDOS Y NOMBRES	TEMA DE TESIS PRIMIGENIO	TEMA DE TESIS MODIFICADO
1	CABREJOS TORRES RAMIRO	INCIDENCIA DE LA METODOLOGÍA MAGERIT V3 EN LA SEGURIDAD DE INFORMACIÓN DE LA EMPRESA DECO INTERIORS SAC	INFLUENCIA DE LA METODOLOGIA MAGERIT V3 EN LA SEGURIDAD DE INFORMACIÓN DE LA EMPRESA DECO INTERIORS SAC.
2	MARRUFO SALAZAR YOAN JOHEL	MEJORA DE LA USABILIDAD Y ACCESIBILIDAD EN PORTALES WEB EN INSTITUCIONES EDUCATIVAS DEL NIVEL SECUNDARIO	EVALUACION DE LA USABILIDAD Y ACCESIBILIDAD EN PORTALES WEB DE INSTITUTOS DE EDUCACIÓN SUPERIOR PEDAGÓGICA DEL PERÚ
3	CAMONES AGUIRRE OSCAR BRYAN	EVALUACION DE LA VIABILIDAD DE IMPLEMENTACION DE TECNICA BASADA EN ALGORITMO GENETICO Y EL FRAMEWORK WS-ATTACKER PARA DETECTAR ATAQUES A SERVICIOS WEB EN UN AMBIENTE DE COMPOSICIÓN DINÁMICO	EVALUACIÓN DE TÉCNICA BASADA EN REGLAS Y ALGORITMO GENÉTICO PARA DETECTAR ATAQUES A SERVICIOS WEB EN UN AMBIENTE DE COMPOSICIÓN DINÁMICO
4	ALVAREZ GONZAGA BRAULIO RICARDO	ANÁLISIS COMPARATIVO DE TÉCNICAS DE EXTRACCIÓN, TRANSFORMACIÓN Y CARGA DE DATOS APLICADAS A BUSINESS INTELLIGENCE	ANÁLISIS COMPARATIVO DE TÉCNICAS DE MINERÍA DE DATOS APLICADAS A BUSINESS INTELLIGENCE
5	SANDOVAL ODAR WILLIAM	COMPARACIÓN DE LAS TÉCNICAS DE SEGMENTACION OPTIMIZACIÓN DE ENJAMBRES DE PARTICULAS Y AGRUPAMIENTO JERÁRQUICO EN AMBIENTES NO CONTROLADOS DE PLANTACIONES DE ARROZ	COMPARACIÓN DE ALGORITMOS DE SEGMENTACION DE IMÁGENES DIGITALES DE PLANTAS DE ARROZ EN AMBIENTES NO CONTROLADOS
6	MOGOLLÓN GARCÍA MANUEL ESTEBAN	EVALUACIÓN DE HERRAMIENTAS DE SEGURIDAD INFORMÁTICA COMO SOPORTE DE LA NORMA ISO 27001 PARA GARANTIZAR LA GESTION DE LA SEGURIDAD DE LA INFORMACIÓN EN UNA MUNICIPALIDAD DEL PERÚ	DESARROLLO DE UN MODELO DE GESTION DE RIESGOS BASADO EN LA METODOLOGÍA MAGERIT PARA MINIMIZAR LOS RIESGOS DE LA IMPLANTACIÓN Y USO DE TI EN UNA MUNICIPALIDAD DEL PERÚ
7	CASTRO FERNÁNDEZ LEVI RONALD	IDENTIFICACIÓN DE INTRUSIONES A BASE DE DATOS DESDE APLICACIONES WEB UTILIZANDO LOS ALGORITMOS DE APRENDIZAJE AUTOMÁTICO	ANÁLISIS COMPARATIVO DE ALGORITMOS DE APRENDIZAJE AUTOMÁTICO PARA IDENTIFICAR ATAQUES DE INYECCIÓN SQL A BASE DE DATOS EN APLICACIONES WEB
8	CALDERON TENORIO CESAR ROLEN	MODELO DE CONTROL AUTOMATICO PARA EL PROCESO DEL RIEGO EN EL CULTIVO DE LA PAPA EN EL CENTRO POBLADO DE CHAQUIL DISTRITO DE LA ESPERANZA PROVINCIA DE SANTA CRUZ REGION DE CAJAMARCA	DESARROLLO DE UN MODELO DE CONTROL AUTOMÁTICO BASADO EN INTELIGENCIA ARTIFICIAL PARA EL PROCESO DEL RIEGO EN EL CULTIVO DE LA PAPA PERUANA