UNIVERSIDAD DE LAMBAYEQUE

FACULTAD DE INGENIERIA

ESCUELA PROFESIONAL DE INGENIERIA DE SISTEMAS

TESIS

PROPUESTA DE UNA AUDITORIA DE SEGURIDAD PARA EL MANEJO DE VULNERABILIDADES DE LA RED INFORMATICA DE LA UNIVERSIDAD SEÑOR DE SIPAN.

PRESENTADA PARA OPTAR EL TÍTULO DE INGENIERO DE SISTEMAS

Autor:

Odar Guerrero Adherly Yeysson Styven

Asesor:

Mgtr. Nauca Torres Enrique Santos

Línea de Investigación:

Gestión de Infraestructura de TI

Chiclayo –Perú

2018

Mgtr. Enrique Santos Nauca Torres
ASESOR

Ing: Segundo José Castillo Zumaran Ortiz
PRESIDENTE

Mgtr: Carlos Antonio Rojas
SECRETARIO

Mgtr. Enrique Santos Nauca Torres
VOCAL

DEDICATORIA

El presente trabajo investigativo lo dedico principalmente a Dios, por ser el inspirador y darme la fuerza para continuar en este proceso de obtener uno de los anhelos más deseados que es mi título.

A mis padres, por su amor, trabajo y sacrificio en todos estos años, gracias a ustedes he logrado llegar hasta aquí y convertirme en lo que soy. Ha sido el orgullo y el privilegio de ser su hijo, son los mejores padres gracias por todo.

A mi hermano por estar siempre presente, acompañándome y por el apoyo moral e incondicional, brindado a lo largo de esta etapa de mi vida.

A todas las personas que me apoyaron y han hecho que el trabajo se realice con éxito en especial a aquellos que nos abrieron las puertas y compartieron sus conocimientos. En el transcurso de la etapa universitaria.

AGRADECIMIENTOS

A DIOS, el que me ha dado fortaleza para continuar cuando he estado a punto de caer, por permitirme llegar a este momento tan especial en mi vida, por los triunfos y los momentos difíciles que me han enseñado a valorarlo cada día más, con toda humildad dedico este trabajo a Dios.

Al finalizar este trabajo quiero utilizar este espacio para agradecer a Dios por todas sus bendiciones, a mis Padres: Manuel de la cruz odar abat y Josefa ida guerrero Ontaneda que han sabido darme su ejemplo de trabajo y honradez a mi hermano maykool odar guerrero por su apoyo y gracias a ellos logre culminar la siguiente tesis.

INDICE

I. INTRODUCCION 12
II. MARCO TEORICO 13
2.1. Antecedentes bibliográficos: 13
2.1.1. En el ámbito internacional.- 13
2.1.2. En el ámbito nacional.- 15
2.1.3. En el ámbito regional.- 16
2.2. Bases teórico 17
2.2.1. La auditoría informática 17
2.2.2. Auditoría informática tiene 2 tipos: 18
2.2.3. Tipos de Auditoría Informática: 20
2.2.4. Importancia de la Auditoría Informática ahora: 21
2.2.5. Principales pruebas y herramientas para efectuar una auditoría informática 21
2.2.6. Áreas a auditar en informática: 21
2.2.7. Los objetivos de una auditoria de seguridad informática son los siguientes: 22
2.2.8. Análisis de riesgos 22
2.2.9.Tipos de auditorías de red: 22
2.2.10. Herramientas para los auditores: 23
2.2.11. Un servicio de auditoría consta de las siguientes fases: 23
2.2.12. Los sistemas de auditoria pueden ser de distinta índole: 24
2.2.13. Metodologías para Auditoría Informática: 25
2.2.14. Octave 25
2.2.15. Magerit - Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información 26
2.2.16. Metodología MAGERIT V3.0 26
2.2.17. D.1. Método de Análisis de Riesgos 31
2.2.18. D.1.3. Determinación Del Impacto Potencial 39
2.2.19. D.1.4. Determinación del Riesgo Potencial 41
2.2.20. D.1.5. Paso 5: Riesgo Residual 50
2.2.21. Herramienta Pilar (7.1.9 - 31.5.2018) 59

2.2.22. Análisis y Gestión de riesgos 59
2.2.23.Criterios de Selección de la Metodología Magerit 60
2.2.24.Criterios de Selección de la Herramienta Pilar 61
2.3. Definición de téminos básicos: 62
2.4. Hipótesis 66
III.MATERIALES Y METODOS 66
3.1. Variables y Operacionalización de Variables 66
3.1.1. Variable única. 66
3.1.2. Operacionalización 66
3.1.3. Objetivos 69
3.1.3.1. Objetivo general. 69
3.1.3.2. Objetivo específicos: 69
3.2. Tipo de estudio, diseño de investigación 69
3.2.1. Investigación Descriptiva – propositiva 69
3.3. Población y muestra de estudio 69
3.3.1. Población: 69
3.3.2. Muestra: 73
3.4. Métodos, técnicas e instrumentos de recolección de datos 74
IV. RESULTADOS 75
4.1. Caracterizar las vulnerabilidades de la red informática de la universidad señor de sipán. 75
4.1.1. Cuestionario de Pregunta: 75
4.1.2. Entrevista. 82
4.2. En base al objetivo: desarrollo: diseñar auditoria de seguridad adaptado a la red informática de la universidad señor de sipán. 82
4.2.1. Se aplica la metodología Magerit mediante: 82
4.2.2. Datos Del Proyecto 84
4.2.3. Método de Análisis de Riesgos 84
4.2.4. MAR 1: Caracterización de los Activos 85
4.2.5. Tarea MAR 1.1: Identificación de los Activos 86
4.2.6. Tarea MAR 1.2: Dependencias entre los Activos 92
4.2.7. Tarea MAR 1.3: Valoración de los Activos 94
4.2.8. MAR 2: Caracterización de las Amenazas 97

4.2.9. Tarea MAR 2.1: Identificación de las Amenazas. 97
4.2.10. Tarea MAR 2.1: Valoración de las Amenazas 99
4.2.11. MAR 3: Caracterización de las Salvaguardas..... 101
4.2.12. Tarea MAR 3.1: Identificación de las Salvaguardas Existentes..... 103
4.2.13. MAR 4: Estimación del Estado de Riesgo..... 106
4.2.14. Tarea MAR 4.1: Estimación del Impacto 107
4.2.15. Tarea MAR 4.2 Estimación del Riesgo 108
4.2.16. Informe..... 114
V. DISCUSION..... 118
VI. CONCLUSIONES..... 119
VII. RECOMENDACIONES 120
VIII. REFERENCIAS BIBLIOGRAFICAS 121
IX. ANEXOS..... 123

INDICE DE TABLAS

TABLA 1: Degradación Del Valor 38
TABLA 2: Probabilidad De Ocurrencia 39
TABLA 3: Comparativa de Metodologías de Análisis y Gestión de Riesgos.....61
TABLA 4: Análisis Comparativo De Las Herramientas AGR. 61
TABLA 5: Población de todas las áreas de la Universidad señor de sipan 73
TABLA 6: Encuesta Pregunta 01.....75
TABLA 7: Encuesta Pregunta 02.....76
TABLA 8: Encuesta Pregunta 03.....77
TABLA 9: Encuesta Pregunta 04.....78
TABLA 10: Encuesta Pregunta 05.....79
TABLA 11: Encuesta Pregunta 06.....80
TABLA 12: Encuesta Pregunta 07.....81
TABLA 13: Diagrama De Dependencia De Activos Según Su Tipo 92
TABLA 14: Tabla De Criterios De Valoración-Pilar 95
TABLA 15: Probabilidad 99
TABLA 16: Degradación.....100
TABLA 17: Aspecto De Las Salvaguardas.....102
TABLA 18: Tipo De Protección De Salvaguarda.....102
TABLA 19: Estimación Del Impacto 107

INDICE DE FIGURAS

Figura 1: ISO 31000 - Marco de trabajo para la gestión de riesgos 27
Figura 2: Elementos del análisis de riesgos potenciales 32
Figura 3: Escala Detallada De Los Criterios De Evaluación..... 36
Figura 4: El Riesgo En Función DEL Impacto y La Probabilidad..... 42
Figura 5: Elementos De Análisis Del Riesgo Residual 45
Figura 6: Tipos De Salvaguardas 48
Figura 7: Eficacia y madurez de las salvaguardas 49
Figura 8: Decisiones de tratamiento de los riesgos..... 54
Figura 9: Zonas De Riesgo 56
Figura 10: Diagrama De Los Proceso De Análisis y Gestión De Riesgos..... 59
Figura 11: Herramienta Pilar - Pantalla de Principal..... 60
Figura 12: Datos Del Proyecto AUDITORIA-USS 83
Figura 13: Datos Del Proyecto AUDITORIA-USS 85
Figura 14: Datos Del Proyecto - AUDITORIA-USS -Activos 86
Figura 15: Lista de Activos - AUDITORIA-USS..... 91
Figura 16: Dependencia De Activos –Auditoria -USS 93
Figura 17: Valoración De Los Activos - AUDITORIA-USS 94
Figura 18: Valoración De Los Activos-Valor Acumulado - AUDITORIA-USS..... 96
Figura 19: Pantalla De Trabajo En El Área De Amenazas. 97
Figura 20: Área De Amenazas. 98
Figura 21: Valoración De Las Amenazas 101
Figura 22: Peso Relativo 103
Figura 23: Impacto Potencial..... 108
Figura 24: Estimación De Riesgo Acumulado 109

Figura 25: Identificación De Riesgos Por Activos 110
Figura 26: Identificación Del Riesgo Crítico Actual 112
Figura 27: Gestión De Seguridad 113
Figura 28: Reducción De Riesgos, Amenazas, Vulnerabilidades y Soluciones . 117

RESUMEN

La presente tesis, propuesta de una auditoria de seguridad para el manejo de vulnerabilidades de la red informática de la universidad señor de sipan., tiene por objetivo un manejo adecuado de vulnerabilidades de la red informática utilizando la herramienta pilar BASIC con una licencia de evaluación de 30 días que se usara para derrollarla realizando un análisis cualitativo de los activos dando lugar a la aplicación del modelo MAGERIT -Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, la cual contribuirá a que la red posea un conocimiento claro sobre las vulnerabilidades que pueden presentarse. MAGERIT fue desarrollado por el Consejo Superior de Administración Electrónica de España, como respuesta al crecimiento acelerado de la tecnología de información y al mayor uso que hacen las Organizaciones, con la finalidad de concientizar a los responsables de los sistemas de información de la existencia de riesgos y de la necesidad de mitigarlos a tiempo. Conclusión En el presente trabajo Se realizó un análisis de riesgos e impactos para ver las vulnerabilidades de la red informática además se describe los conceptos e importancia relacionada en la auditoria informática de seguridad de los diversos equipos, servicios y personal del área de TI con el uso de la herramienta pilar utilizando la metodología Magerit enfocándose en los activos de toda la red para ver y diagnosticar su estado actual. Se recomienda realizar anualmente una auditoria para ver el estado actual de los equipos y su funcionamiento para que brinden un correcto servicio y que no estén vulnerables a los daños tanto físicos como lógicos por lo tanto se, logra así tener todo bajo control y toda la seguridad de su base de datos.

Palabras Claves: Herramienta pilar, Magerit, Vulnerabilidades.

ABSTRACT

The present thesis, proposal of a security audit for the management of vulnerabilities of the computer network of the Lord of Sipan University., Aims at an adequate management of vulnerabilities in the computer network using the BASIC pillar tool with an evaluation license of 30 days that will be used to defeat it by carrying out a qualitative analysis of the assets, leading to the application of the MAGERIT model - Methodology of Analysis and Risk Management of Information Systems, which will contribute to the network having a clear knowledge about vulnerabilities that can be presented. MAGERIT was developed by the Superior Council of Electronic Administration of Spain, in response to the accelerated growth of information technology and the increased use made by Organizations, with the aim of raising awareness among those responsible for information systems of the existence of risks and the need to mitigate them in time. Conclusion In the present work an analysis of risks and impacts was performed to see the vulnerabilities of the computer network, and the concepts and importance related to the security audit of the various IT equipment, services and personnel are described with the use of the pillar tool using the Magerit methodology focusing on the assets of the entire network to see and diagnose its current status. It is recommended to conduct an annual audit to see the current status of the equipment and its operation so that they provide a correct service and that they are not vulnerable to physical and logical damage, therefore, they are able to have everything under control and all the security from your database.

Key words: Pilar tool, Magerit, Vulnerabilities.

I. INTRODUCCION

El presente proyecto se realizó A través de las encuestas y entrevistas aplicadas, se determinó diversos problemas y vulnerabilidades que tiene en la actualidad, entre los principales problemas hallamos las políticas de seguridad, el mal funcionamiento del servicio de internet ,no tiene respaldo de bakup y el sistema que se encuentra vulnerable ante cualquier ataque que se presentan a diario en las diferentes áreas de la red informática de la universidad señor de sipan, Además se identificó que el personal TI no tiene conocimiento de todos los problemas que existen en las diferentes áreas , cómo funciona cada proceso y esto se debe a que no se existen mecanismos de seguridad que permitan proteger la integridad de la información de la de la red informática

Como objetivo general de la presente tesis tenemos: proponer una auditoria de seguridad para el manejo de vulnerabilidades de la red informática de la Universidad Señor de Sipán y los objetivos específicos son: Caracterizar las vulnerabilidades de la red informática de la Universidad Señor de Sipán y Diseñar auditoria de seguridad adaptado a dicha red informática utilizando la Herramienta Pilar (7.1.9 31.5.2018).con las metodología Magerit.

Al aplicar esta auditoría, permitirá aumentar la eficiencia y eficacia en el desarrollo de las operaciones, haciendo los procedimientos más seguros y brindando mayor agilidad de las actividades para las diferentes áreas que se brinda el servicio como para usuarios internos y externos de la red informática así como ver las vulnerabilidades que tiene para darle solución y utilizar salvaguardas para mitigar los daños posibles que puedan ocurrir.

Para el presente proyecto, se hizo un estudio de análisis cuantitativo en la herramienta pilar (7.1.9 31.5.2018).se usó con una licencia de evaluación y con la metodología Magerit que utiliza la iso 27002-2013.se realiza este proceso ingresando todos los activos logrando así una auditoria de seguridad entonces habrá un manejo adecuado de vulnerabilidades de la red informática de la universidad señor de sipan

Posteriormente se utilizan las salvaguardas que la herramienta pilar da para mitigar las vulnerabilidades encontradas y así dar solución a los problemas encontrados.

II. MARCO TEORICO

2.1. **Antecedentes bibliográficos:**

2.1.1. **En el ámbito internacional.-**

1. (larrea Bustos & Yangua Jumbo, 2014) En su investigación denominada "Auditoría Informática y su Incidencia en los Riesgos para el manejo de la Información en la Cooperativa de Ahorro y Crédito Educadores de Tungurahua", cuyo objetivo es (Determinar de qué manera la ineficiente Auditoría Informática influye en los riesgos para el manejo de la información en la Cooperativa de Ahorro y Crédito Educadores de Tungurahua.) el diseño de la investigación fue(bibliográfica-documental)los métodos utilizados fueron(la observación, entrevista, Análisis documentario) los resultados obtenidos(es tener conocimiento de cómo se encuentra la empresa actualmente, y en que es lo que están fallando para mejorar su desempeño tanto técnico, científico, y humano; ya que uno de los objetivos propuestos de la entidad es tener un gran rendimiento y progreso ante la dura competencia que se da día tras día, por lo que ayuda a que cada empresa tome medidas preventivas ante cualquier situación que se le presente y así no tener mayores problemas ene l futuro.).las conclusiones indican que(La mayoría de los empleados tienden a utilizar la misma contraseña de seguridad y la comparten con personas de su confianza, lo cual causaría graves problemas en la Seguridad de la Información y conduciría una falta de control de Seguridad dentro de la Empresa ya que esta puede ser robada y por ello pueden tener acceso a todas sus cuentas sin necesidad de hacer mayor esfuerzo para lograr objetivos maliciosos.).Finalmente recomienda que (Aplicar estrategias como dar charlas sobre los grandes peligros que conlleva el compartir la contraseña de Seguridad con diferentes personas causando un alto riesgo en la Seguridad en los Departamentos de la Empresa.) .

   Comentario.-la relevancia que tiene esta investigación para la tesis El desconocimiento que existe con respecto a los riesgos para el manejo de la información acarrearía consecuencias trágicas si no se previene antes y

se da valor a la importancia que tiene la información que se maneja interna y externa.

2. (Ruiz Banda & Acosta Jordán, 2016)En su investigación denominada “Auditoría informática para la optimización del funcionamiento del de los sistemas informáticos de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial”, cuyo objetivo es (Realizar una Auditoría Informática para optimizar el funcionamiento de los sistemas y equipos informáticos de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial) el diseño de la investigación fue (bibliográfica-documental) los métodos utilizados fueron(la entrevista ,análisis de datos) los resultados obtenidos(La aplicación de pruebas sustantivas y de cumplimiento pudo demostrar que los equipos informáticos tienen un buen funcionamiento y son de gran utilidad para los estudiantes de la Facultad, las herramientas de hardware y software son estudiados e instalados al inicio de cada semestre según las necesidades cada laboratorio de las diferentes carreras).las conclusiones indican que(La aplicación de pruebas sustantivas y de cumplimiento pudo demostrar que los equipos informáticos tienen un buen funcionamiento y son de gran utilidad para los estudiantes de la Facultad, las herramientas de hardware y software son estudiados e instalados al inicio de cada semestre según las necesidades cada laboratorio de las diferentes carreras.)finalmente recomienda que (se recomienda utilizar el sistema con el propósito para el que fue creado, evitando justificar faltas y atrasos sin documentación que lo prueben, con el fin de que el sistema presente resultados reales de las jornadas diarias) .

   Comentario.-la relevancia que tiene esta investigación para la tesis El desconocimiento que existe con respecto a los riesgos en las diferentes áreas con el manejo de la información acarrearía consecuencias trágicas cuando usan las mismas contraseñas para realiza sus actividades lo cual genera una mala gestión de información que se maneja.

3. (Ulloa Barrera, 2017) En su investigación denominada “Auditoría informática aplicando la metodología COBIT en el Gobierno Autónomo Descentralizado

Municipal de San Cristóbal de Patate.", cuyo objetivo es (Realizar una auditoría informática aplicando la metodología COBIT en el Gobierno Autónomo Descentralizado Municipal de San Cristóbal de Patate) el diseño de la investigación fue(investigación de campo)los métodos utilizados fueron(entrevista, encuesta)los resultados obtenidos().las conclusiones indican que(Mediante el marco de referencia COBIT, se ha evaluado los sistemas de las Tecnologías de la información (TI), es decir identificar riesgos, gestión de recursos y medir desempeño, asegurando un servicio continuo, efectivo, eficiente y confiable.) finalmente recomienda que (El GAD Municipal de San Cristóbal de Patate, debe tomar una mayor consideración a los procesos que tuvieron un nivel de madurez de nivel cero:PO9 Evaluar los riesgos, DS7 Educar y capacitar usuarios, M2 evaluar qué tan adecuado es el Control Interno).

Comentario.-la relevancia que tiene esta investigación para la tesis es que nos da un alcance de los riesgos que se pueden identificar realizando una auditoria y con una buena metodología que es cobit con el cual miden el desempeño de la organización.

2.1.2. **En el ámbito nacional.-**

1. (fukumoto, 2017)En su investigación denominada "sistema web para la mejora en el tiempo de respuesta de las reclamaciones de clientes y hacia proveedores, y auditorías en planta agroindustrial de Green Perú s.a.", cuyo objetivo es (Determinar la mejora en el tiempo de respuesta de las reclamaciones de clientes y hacia proveedores, y auditorías en Planta Agroindustrial de Green Perú S.A. mediante el desarrollo de un sistema web.) el diseño de la investigación fue(ágil)los métodos utilizados fueron(análisis de datos) los resultados obtenidos(Como resultado de la segunda iteración del proyecto llevado a cabo, los clientes quedaron satisfechos con la funcionalidad e integración de los módulos desarrollados, ya que con estos últimos contará con los reportes necesarios para la mejora en el tiempo de respuesta a las reclamaciones de clientes y proveedores, y auditorías.).Las conclusiones indican que (Se ha desarrollado un sistema web para reducir los errores en un 80% con respecto

a la información brindada de los insumos utilizados. Además se puede acceder a la información de manera rápida y compartida.) Finalmente recomienda que (Desarrollar un sistema para el control y manejo de los productos fabricados diariamente, los pedidos solicitados, los pedidos despachados y los pedidos pendientes por fabricar y despachar).

2. (Moises, 2017)En su investigación denominada “auditoría informática para el área de gestión de créditos del banco financiero – oficina Chimbote”, cuyo objetivo es (es mejorarlos procesos que se realizan en el Banco Financiero Sede Chimbote y con mayor enfoque en el área de crédito aplicando una auditoría informática. Para ello se utilizó el estándar COBIT como modelo que permitirá auditar la gestión y control de los sistemas de información y tecnología.) El diseño de la investigación fue (propositiva-experimental)los métodos utilizados fueron(encuestas ,checklist, cuestionarios) los resultados obtenidos(se logró verificar el incremento de la satisfacción de los clientes del Banco Financiero Sede Chimbote y también generar un plan de acción con las posibles mejoras en los proceso no sólo del área de crédito que permitirán asegurar una mayor integridad, confidencialidad y confiabilidad de la información. También se pudo realizar la viabilizarían económica del presente proyecto.).Las conclusiones indican que (Se Analizó el contexto en el que actúa el Banco Financiero Sede Chimbote y sobre todo el área de gestión de crédito a través de información recolectada, entrevistas, plan estratégico de la institución, manuales de procedimiento y reglamentos.) finalmente recomienda que (Incrementar el uso de las redes sociales para publicitar los procesos de crédito como Facebook, twitter, para que no solo sea por llamadas telefónicas o página web. Además poner publicidad en televisión y radio con las más altas sintonías.).

2.1.3. **En el ámbito regional.-**

1. (Campos Muños & Rios Damian, 2016) En su investigación denominada “auditoría en el uso de tecnología de información para optimizar la seguridad de la caja sipán s.a”, cuyo objetivo es (Determinar de qué manera la ineficiente Auditoría Informática influye en los riesgos para el manejo de la información en la Cooperativa de Ahorro y Crédito Educadores de

Tungurahua) el diseño de la investigación fue(investigación en campo)los métodos utilizados fueron(entrevistas a personas expertas) los resultados obtén Confianza en los usuarios sobre la seguridad y control de los servicios de TI y Optimiza las relaciones internas y del clima de trabajo idos().las conclusiones indican que(Se realizó el levantamiento de información para conocer la estructura orgánica del área de Tecnología de Información de la Caja Sipán, determinando que existe un Comité de Riesgos como órgano staff asesor al Directorio de la Caja; además de un Área de Tecnologías de Información con jefe encargado, jefe de desarrollo y mantenimiento, responsable de producción y soporte técnico, y jefe de organización y método; concordante con lo estipulado en el Art. N°4 del Circular G-140-2009-SBS y en la normatividad Resolución S.B.S. N°2116 -2009) finalmente recomienda que (Se recomienda realizar auditorías específicas para cada proceso o recurso de tecnología de información como por ejemplo de base de datos, de comunicaciones, de seguridad física, de seguridad lógica, de los programas).

2.2. **Bases teórico**

2.2.1. **La auditoría informática**

Es un proceso llevado a cabo por profesionales especialmente capacitados para el efecto, y que consiste en recoger, agrupar y evaluar evidencias para determinar si un Sistema de Información salvaguarda el activo empresarial, mantiene la integridad de los datos ya que esta lleva a cabo eficazmente los fines de la organización, utiliza eficientemente los recursos, cumple con las leyes y regulaciones establecidas. Permiten detectar de Forma Sistemática el uso de los recursos y los flujos de información dentro de una Organización y determinar qué Información es crítica para el cumplimiento de su Misión y Objetivos, identificando necesidades, falsedades, costes, valor y barreras, que obstaculizan flujos de información eficientes (Gomez Ramirez, Evaluación de la seguridad de la información con la metodología Octave, 2014).

2.2.2. **Auditoría informática tiene 2 tipos:**

A. Auditoria Interna**:** Es aquella que se hace desde dentro de la empresa; sin contratar a personas ajenas, en el cual los empleados realizan esta auditoría trabajan ya sea para la empresa que fueron contratados o simplemente algún afiliado a esta.

B. Auditoria Externa**:** Como su nombre lo dice es aquella en la cual la empresa contrata a personas de afuera para que haga la auditoría en su empresa. Auditar consiste principalmente en estudiar los mecanismos de control que están implantados en una empresa u organización, determinando si los mismos son adecuados y cumplen unos determinados objetivos o estrategias, estableciendo los cambios que se deberían realizar para la consecución de los mismos.

1. **Los mecanismos de control en el área de Informática son:**

Directivos, preventivos, de detección, correctivos o de recuperación ante una contingencia.

2. **Los objetivos de la auditoría Informática son:**

El análisis de la eficiencia de los Sistemas Informáticos

La verificación del cumplimiento de la Normativa en este ámbito

La revisión de la eficaz gestión de los recursos informáticos.

3. **También existen otros tipos de auditoria**

Auditoría operacional**:** se refiere a la revisión de la operación de una empresa y juzga la eficiencia de la misma.

Auditoría administrativa: se refiere a la organización y eficiencia de la estructura del personal con la que cuenta el personal y los procesos administrativos en que actúa dicho personal

Auditoría social: se refiere a la revisión del entorno social en que se ubica y desarrolla una empresa, con el fin de valorar aspectos externos e internos que interfieren en la productividad de la misma.

4. Sus beneficios son:

Mejora la imagen pública Confianza en los usuarios sobre la seguridad y control de los servicios de TI.

1. Optimiza las relaciones internas y del clima de trabajo.
2. Disminuye los costos de la mala calidad (reprocesos, rechazos, reclamos, entre otros).
3. Genera un balance de los riesgos en TI.
4. Realiza un control de la inversión en un entorno de TI, a menudo impredecible.
5. La auditoría informática sirve para mejorar ciertas características en la empresa como:

Desempeño:

1. Fiabilidad
2. Eficacia
3. Rentabilidad
4. Seguridad
6. Privacidad

Generalmente se puede desarrollar en alguna o combinación de las siguientes:

Áreas:

1. Gobierno corporativo
2. Administración del Ciclo de vida de los sistemas
3. Servicios de Entrega y Soporte
4. Protección y Seguridad
5. Planes de continuidad y Recuperación de desastres

La necesidad de contar con lineamientos y herramientas estándar para el ejercicio de la auditoría informática ha promovido la creación y desarrollo de mejores prácticas como COBIT, COSO e ITIL.

Actualmente la certificación de ISACA para ser CISA Certified Information Systems Auditor es una de las más reconocidas y avaladas por los estándares internacionales

ya que el proceso de selección consta de un examen inicial bastante extenso y la necesidad de mantenerse actualizado acumulando horas (puntos) para no perder la certificación.

2.2.3. **Tipos de Auditoría Informática:**

Dentro de la auditoría informática destacan los siguientes tipos (entre otros):

1. Auditoría de la gestión**:** la contratación de bienes y servicios, documentación de los programas, etc.
2. Auditoría legal del Reglamento de Protección de Datos: Cumplimiento legal de las medidas de seguridad exigidas por el Reglamento de desarrollo de la Ley Orgánica de Protección de Datos.
3. Auditoría de los datos: Clasificación de los datos, estudio de las aplicaciones y análisis de los flujogramas.
4. Auditoría de las bases de datos: Controles de acceso, de actualización, de integridad y calidad de los datos.
5. Auditoría de la seguridad: Referidos a datos e información verificando disponibilidad, integridad, confidencialidad, autenticación y no repudio.
6. Auditoría de la seguridad física**:** Referido a la ubicación de la organización, evitando ubicaciones de riesgo, y en algunos casos no revelando la situación física de esta. También está referida a las protecciones externas (arcos de seguridad, CCTV, vigilantes, etc.) y protecciones del entorno.
7. Auditoría de la seguridad lógica: Comprende los métodos de autenticación de los sistemas de información.
8. Auditoría de las comunicaciones**.** Se refiere a la auditoría de los procesos de autenticación en los sistemas de comunicación.
9. Auditoría de la seguridad en producción: Frente a errores, accidentes y fraudes.

2.2.4. **Importancia de la Auditoría Informática ahora:**

La auditoría permite a través de una revisión independiente, la evaluación de actividades, funciones específicas, resultados u operaciones de una organización, con el fin de evaluar su correcta realización. Este autor hace énfasis en la revisión independiente, debido a que el auditor debe mantener independencia mental, profesional y laboral para evitar cualquier tipo de influencia en los resultados de la misma. La técnica de la auditoría, siendo por tanto aceptables equipos multidisciplinarios formados por titulados en Ingeniería Informática e Ingeniería Técnica en Informática y licenciados en derecho especializados en el mundo de la auditoría.

2.2.5. **Principales pruebas y herramientas para efectuar una auditoría informática**

En la realización de una auditoría informática el auditor puede realizar las siguientes pruebas:

A. Pruebas sustantivas: Verifican el grado de confiabilidad del SI del organismo. Se suelen obtener mediante observación, cálculos, muestreos, entrevistas, técnicas de examen analítico, revisiones y conciliaciones. Verifican asimismo la exactitud, integridad y validez de la información.

B. Pruebas de cumplimiento: Verifican el grado de cumplimiento de lo revelado mediante el análisis de la muestra. Proporciona evidencias de que los controles claves existen y que son aplicables efectiva y uniformemente.

2.2.6. **Áreas a auditar en informática:**

Las áreas a auditar en donde se puede realizar la auditoría informática, puede ser:

A toda la entidad

A una función

A una subfuncion

Se pueden aplicar los siguientes tipos de auditoría:

Auditoría al ciclo de vida del desarrollo de un sistema

2.2.7. **Los objetivos de una auditoria de seguridad informática son los siguientes:**

1. Verificar si el sistema de seguridad implantado cumple con la finalidad de proteger el sistema informático.
2. Detectar vulnerabilidades y amenazas.
3. Hacer un informe detallado con los resultados y un plan de acciones para mejorar.

2.2.8. **Análisis de riesgos**

Para identificar los elementos del sistema informático pasan por estas fases:

Inventario y valoración de los activos de la organización.

1. Identificar y valorar las amenazas y las vulnerabilidades.
2. Definir sistemas de medición de riesgos.
3. Determinar el impacto y el riesgo de un ataque.
4. Identificar y evaluar las medidas de seguridad existentes.

Una manera de realizar una auditoria es mediante el test de penetración o intrusión en el cual son los propios auditores los que intentan romper los sistemas de seguridad de manera autorizada (Seguridad Informática Isidro, s.f.) .

2.2.9. **Tipos de auditorías de red:**

1. Auditoria de red interna: Se contrasta el nivel de seguridad y privacidad e redes locales internas sin tener en cuenta Internet.
2. Auditoria perimetral y DMZ: Se realiza desde Internet para evaluar el grado de protección que tenemos frente a ataques externos. Se evalúa tanto la protección de la red interna como de la DMZ.
3. Test de intrusión: Se utiliza una base de datos de vulnerabilidades conocidas para generar un informe sobre ellas.
4. Auditoria de aplicaciones: Se testean los programas utilizados sin tener en cuenta los servidores o sistemas operativos. Se hacen pruebas de desbordamiento de buffer, inyección SQL, etc...

5. Análisis forense: Se separa la maquina atacada de la red y se analiza para ver que ha ocurrido para evitar incidentes similares. Se trata de reconstruir como se ha penetrado en el sistema y se valoran los daños.

2.2.10. **Herramientas para los auditores:**

Enumeración de redes: Su objetivo es identificar las redes IP asociadas a una empresa y descubrir sus servidores, esta información se puede obtener a través el "whois" y los DNS.

Rastreo de redes: Se utilizan barridos de direcciones IP con ICMP, barrido de puertos TCP y UDP e identificar sistema operativo y aplicaciones. Su objetivo es obtener más información sobre las redes de la empresa y una de las herramientas más utilizadas es NMAP, es decir, con NMAP se pueden hacer rastreos de puertos, etc...

Barrido de puertos: Trata de identificar los puertos TCP y UDP abiertos para entrar en el sistema aprovechando los servicios que lo utilizan. Suele ser lo primero que realizan los atacantes.

Finger-printing: Son técnicas para identificar el sistema operativo de los servidores y las versiones de las aplicaciones utilizadas, se suele utilizar NMAP junto a Wireshark.

Análisis de vulnerabilidades: El objetivo es detectar vulnerabilidades y corregirlas, se pueden utilizar las siguientes herramientas: Nessus, Openvas, etc...

Test de penetración: Algunas herramientas son: SignSploit, MetaSploit, etc...

Una auditoría de seguridad informática es la evaluación de los sistemas informáticos llevado a cabo por profesionales para identificar, enumerar y describir las vulnerabilidades que puedan haber en las estaciones de trabajo, redes de comunicaciones y/o servidores (Germain, 2017).

2.2.11. **Un servicio de auditoría consta de las siguientes fases:**

1. Enumeración de redes, topologías y protocolos.
2. Verificación del cumplimiento de los estándares internacionales: ISO, COBIT…
3. Identificación de los Sistemas Operativos instalados.

4. Análisis de servicios y aplicaciones.
5. Detección, comprobación y evaluación de vulnerabilidades.
6. Medidas específicas de corrección.

Con los resultados obtenidos, se reporta un informe con las medidas preventivas que deben tomar los administradores para mejorar la seguridad de sus sistemas. Las auditorías permiten conocer en el momento que se realizan la situación exacta de las medidas de seguridad de la empresa.

Las empresas deben tener un plan de emergencia ante posibles desastres, implementando una metodología en caso que ocurra alguna vulnerabilidad. Hay que instalar un sistema apoyado en herramientas de análisis y verificación que permitan determinar las debilidades y posibles fallos para repararlos inmediatamente o frenar el ataque. Aparte de la Auditoria de Seguridad, se debe realizar un mantenimiento para asegurar la integridad de los controles de seguridad. Se necesitan parches, actualizaciones y nuevos productos.

2.2.12. **Los sistemas de auditoria pueden ser de distinta índole:**

1. **Auditoria de seguridad interna:** Se contrasta el nivel de seguridad y privacidad de las redes locales y corporativas de carácter interno.
2. **Auditoria de seguridad perimetral:** Se analiza el grado de seguridad de la red local o corporativa en las entradas exteriores
3. **Test de intrusión:** Se intenta acceder a los sistemas para comprobar el nivel de resistencia a una intrusión no deseada.
4. **Análisis forense:** Estudio posterior a un incidente, en el cual se trata de reconstruir cómo se ha penetrado en el sistema y se valoran los daños ocasionados.
5. **Auditoría de páginas web**: Se comprueban las vulnerabilidades de una página web.
6. **Análisis de código:** Tanto de aplicaciones como de páginas web.

2.2.13. **Metodologías para Auditoría Informática:**

La auditoría informática es una parte fundamental de la Seguridad Computacional que permite medir y controlar riesgos informáticos que pueden ser aprovechados por personas o sistemas ajenos a nuestra organización o que no deben tener acceso a nuestros datos. En este sentido, identificar los riesgos de manera oportuna ayudará a implementar de manera preventiva, las medidas de seguridad. Para facilitar esta actividad, existen diferentes metodologías que ayudan en el proceso de revisión de riesgos informáticos. Dos de las más utilizadas son Octave y Magerit.

2.2.14. **Octave**

La metodología Octave es una evaluación que se basa en riesgos y planeación técnica de seguridad computacional. Es un proceso interno de la organización, significa que las personas de la empresa tienen la responsabilidad de establecer la estrategia de seguridad una vez que se realice dicha evaluación, y es precisamente lo interesante de esta metodología que la evaluación se basa en el conocimiento del personal de la empresa para capturar el estado actual de la seguridad. De esta manera es más fácil determinar los riesgos críticos.

A diferencia de las evaluaciones típicas enfocadas en la tecnología, OCTAVE está dirigida a riesgos organizacionales y está enfocada en temas estratégicos relacionados con la práctica, es flexible y puede aplicarse a la medida para la mayoría de las organizaciones. En esta revisión es necesario que las empresas manejen el proceso de la evaluación y tomen las decisiones para proteger la información. El equipo de análisis, integrado por personas de los departamentos de TI, de negocios, etc, lleva a cabo la evaluación, debido a que todas las perspectivas son cruciales para controlar los riesgos de seguridad computacional (Gomez Ramirez, Evaluación de la seguridad de la información con la metodología Octave, 2014).

2.2.15. Magerit - Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información

La metodología Magerit fue desarrollada en España debido al rápido crecimiento de las tecnologías de información con la finalidad de hacerle frente a los diversos riesgos relacionados con la seguridad informática.

La CSAE (Consejo Superior de Administración Electrónica) promueve la utilización de esta metodología como respuesta a la creciente dependencia de las empresas para lograr sus objetivos de servicio.

1. **Las faces que contempla el modelo Magerit son:**

   B. Planificación del Proyecto.- establece el marco general de referencia para el proyecto.
   C. Análisis de Riesgos.- permite determinar cómo es, cuánto vale y cómo están protegidos los activos.
   D. Gestión de Riesgos.- permite la selección e implantación de salvaguardas para conocer, prevenir, impedir, reducir o controlar los riesgos identificados".

   Al aplicar esta metodología se conocerá el nivel de riesgo actual de los activos, y por lo tanto se podrá mejorar las aplicaciones de salvaguardas y se podrá conocer el riesgo reducido o residual. La razón de ser de MAGERIT está directamente relacionada con la generalización del uso de los medios electrónicos, informáticos y telemáticos, que supone unos beneficios evidentes para los ciudadanos, pero que también da lugar a ciertos riesgos que deben minimizarse con medidas de seguridad que garanticen la autenticación, confidencialidad, integridad y disponibilidad de los sistemas de información y generan confianza cuando se utilicen tales medios.2

   Inclusive, se ha desarrollado software como Pilar basado en la metodología de Magerit (Lucero Gomez, 2012).

2.2.16. Metodología MAGERIT V3.0

MAGERIT es la metodología de análisis y gestión de riesgos de los Sistemas de Información elaborada por el Consejo Superior de Administración Electrónica

(CSAE), Ministerio De Hacienda Y Administración Pública — Gobierno De España, como respuesta a la percepción de que la Administración y en general toda la sociedad, dependen de forma creciente de las tecnologías de la información para el cumplimiento de su misión.

La razón de ser de MAGERIT está directamente relacionada con la generalización del uso de las tecnologías de la información, que supone unos beneficios evidentes para los ciudadanos; pero también da lugar a ciertos riesgos que deben minimizarse con medidas de seguridad que generen confianza.

MAGERIT interesa a todos aquellos que trabajan con información digital y sistemas informáticos para tratarla. Si dicha información, o los servicios que se prestan gracias a ella, son valiosos, MAGERIT les permitirá saber cuánto valor está en juego y les ayudará a protegerlo. Conocer el riesgo al que están sometidos los elementos de trabajo es, simplemente, imprescindible para poder gestionarlos. Con MAGERIT se persigue una aproximación metódica que no deje lugar a la improvisación, ni dependa de la arbitrariedad del analista.

Siguiendo la terminología de la normativa ISO 31000, MAGERIT responde a lo que se denomina “Proceso de Gestión de los Riesgos”, sección 4.4 (“implementación de la Gestión de los Riesgos”) dentro del “Marco de Gestión de Riesgos”. En otras palabras, MAGERIT implementa el Proceso de Gestión de Riesgos dentro de un marco de trabajo para que los órganos de gobierno tomen decisiones teniendo en cuenta los riesgos derivados del uso de tecnologías de la información.

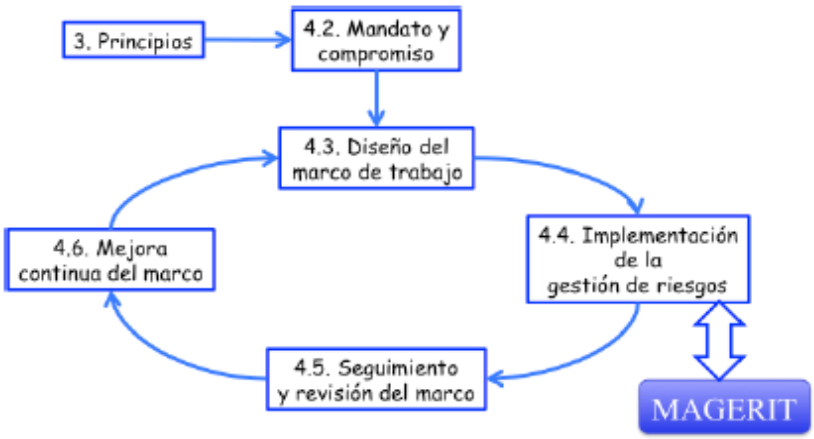


Figura 1: ISO 31000 - Marco de trabajo para la gestión de riesgos

Fuente: (MAGERIT -- version 3.0.Libro Libro I:Metodo publicas, Gobierno de España-Ministerio De Hacienda y Relaciones, 2012)

A. Objetivos

MAGERIT persigue los siguientes objetivos:

B.1. Directos

Concientizar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos.

Ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC).

Ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control.

B.2. Indirectos

Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso

B. Organización de las Guías

Esta versión 3 de Magerit se ha estructurado en dos libros y una guía de técnicas:

Libro l: Método

Libro ll: Catálogo de elementos

Guía de Técnicas: Recopilacion de técnicas de diferente tipo que pueden ser de utilidad para la aplicación del método.

1. **C.1. Libro I**

Este libro se estructura de la siguiente forma:

Capítulo 2

Presenta los conceptos informalmente. En particular se enmarcan las actividades de análisis y tratamiento dentro de un proceso integral de gestión de riesgos.

Capítulo 3

Concreta los pasos y formaliza las actividades de análisis de los riesgos.

Capítulo 4

Describe opciones y criterios de tratamiento de los riesgos y formaliza las actividades de gestión de riesgos.

Capítulo 5

Se centra en los proyectos de análisis de riesgos, proyectos en los que nos veremos inmersos para realizar el primer análisis de riesgos de un sistema y eventualmente cuando hay cambios sustanciales y hay que rehacer el modelo ampliamente.

Capítulo 6

Formaliza las actividades de los planes de seguridad, a veces denominados planes directores o planes estratégicos.

Capítulo 7

Se centra en el desarrollo de sistemas de información y cómo el análisis de riesgos sirve para gestionar la seguridad del producto final desde su concepción inicial hasta su puesta en producción, así como a la protección del propio proceso de desarrollo.

Capítulo 8

Se anticipa a algunos problemas que aparecen recurrentemente cuando se realizan análisis de riesgos.

Los apéndices recogen material de consulta:

1. Un glosario.
2. Referencias bibliográficas consideradas para el desarrollo de esta metodología,
3. Referencias al marco legal que encuadra las tareas de análisis y gestión en la Administración Pública Española.
4. El marco normativo de evaluación y certificación.

5. Las características que se requieren de las herramientas, presentes o futuras, para soportar el proceso de análisis y gestión de riesgos.
6. Una guía comparativa de cómo Magerit versión 1 ha evolucionado a la versión 2 y a esta versión 3.

2. **C.2. Libro II**

En libro aparte, se propone un catálogo, abierto a ampliaciones, que marca unas pautas en cuanto a:

Tipos de activos

Dimensiones de valoración de los activos

Criterios de valoración de los activos

Amenazas típicas sobre los sistemas de información

Salvaguardas a considerar para proteger sistemas de Information

Se persiguen dos objetivos:

1. Por una parte, facilitar la labor de las personas del proyecto, en el sentido de ofrecerles elementos estándar a los que puedan describirse rápidamente, centrándose en lo específico del sistema objeto del análisis.

2. Por otra, homogeneizar los resultados de los análisis, promoviendo una terminología y unos criterios uniformes que permitan comparar e incluso integrar análisis realizados por diferentes equipos.

C.3. Guía de Técnicas

En libro aparte, aporta luz adicional y orientación sobre algunas técnicas que se emplean habitualmente para llevar a cabo proyectos de análisis y gestión de riesgos:

Técnicas específicas para el análisis de riesgos

a. Análisis mediante tablas
b. Análisis algorítmico
c. Arboles de ataque

d. Técnica general

e. Técnicas gráficas

f. Sesiones de trabajo: entrevistas, reuniones y presentaciones

g. Valoración Delphi Se trata de una guía de consulta.

Según el lector avance por las tareas del proyecto, se le recomendará el uso de ciertas técnicas específicas, de las que esta guía busca ser una introducción, así como proporcionar referencias para que el lector profundice en las técnicas presentadas.

Método de Análisis de Riesgos y Proceso de Gestión de Riesgos

2.2.17. **D.1. Método de Análisis de Riesgos**

El análisis de riesgos es una aproximación metódica para determinar el riesgo siguiendo unos pasos pautados:

1. Determinar los activos relevantes para la Organización, su interrelación y su valor, en el sentido de qué perjuicio (coste) supondría su degradación.
2. Determinar a qué amenazas están expuestos aquellos activos.
3. Determinar qué salvaguardas hay dispuestas y cuán eficaces son frente al riesgo.
4. Estimar el impacto, definido Como el daño sobre el activo derivado de la materialización de la amenaza.
5. Estimar el riesgo, definido Como el impacto ponderado con la tasa de ocurrencia (o expectativa de materialización) de la amenaza.

Con el objeto de organizar la presentación, se introducen los conceptos de "impacto y riesgo potenciales" entre los pasos 2 y 3. Estas valoraciones son "teóricas": en el caso de que no hubiera salvaguarda alguna desplegada. Una vez obtenido este escenario teórico, se incorporan las salvaguardas del paso 3, derivando estimaciones realistas de impacto y riesgo. La siguiente figura recoge este primer recorrido, cuyos pasos se detallan en las siguientes secciones:

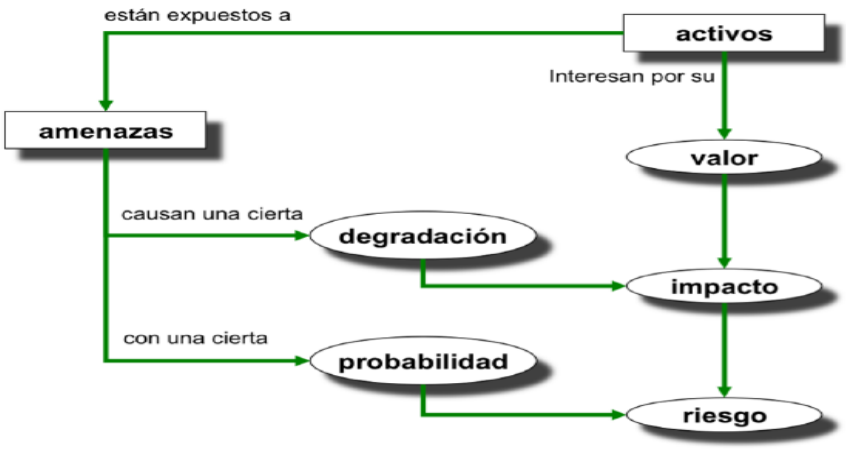


Figura 2: Elementos del análisis de riesgos potenciales

Fuente: (MAGERIT -- version 3.0.Libro Libro I:Metodo publicas, Gobierno de España-Ministerio De Hacienda y Relaciones, 2012)

1. D.1.1. Paso 1: Activos

Componente o funcionalidad de un sistema de información susceptible de ser atacado accidentalmente con consecuencias para la organización, incluye:

En un sistema de información hay 2 cosas esenciales: La información que maneja

Los servicios que presta.

Estos activos esenciales marcan los requisitos de seguridad para todos los demás componentes del sistema.

Datos que materializan la información.

Servicios auxiliares que se necesitan para poder organizar el sistema.

Las aplicaciones informáticas (software) que permiten manejar los datos.

Los equipos informáticos (hardware) y que permiten hospedar datos, aplicaciones y servicios.

Los soportes de información que son dispositivos de almacenamiento de datos. El equipamiento auxiliar que complementa el material informático.

Las redes de comunicaciones que permiten intercambiar datos.

Las instalaciones que acogen equipos informáticos y de comunicaciones.

Las personas que explotan u operan todos los elementos anteriormente citados.

1. **Dependencias**

Los activos esenciales son la información y los servicios prestados; pero estos activos dependen de otros activos más prosaicos como pueden ser los equipos, las comunicaciones, las instalaciones y las frecuentemente olvidadas personas que trabajan con aquellos.

De manera que los activos vienen a formar árboles o grafos de dependencias donde la seguridad de los activos que se encuentran más arriba en la estructura o 'superiores' depende de los activos que se encuentran más abajo o 'inferiores'. Estas estructuras reflejan de arriba hacia abajo las dependencias, mientas que de abajo hacia arriba la propagación del daño caso de materializarse de las vulnerabilidades.

Aunque en cada caso hay que adaptarse a la Organización objeto del análisis, con frecuencia se puede estructurar el conjunto de activos en capas, donde las capas superiores dependen de las inferiores:

2. **Valoración**

Por qué interesa un activo7 Por lo que vale.

No se está hablando de lo que cuestan las cosas, sino de lo que valen. Si algo no vale para nada, prescíndase de ello. Si no se puede prescindir impunemente de un activo, es que algo vale; eso es lo que hay que averiguar pues eso es lo que hay que proteger.

La valoración se puede ver desde la perspectiva de la 'necesidad de proteger' pues cuanto más valioso es un activo, mayor nivel de protección requeriremos en la dimensión (o dimensiones) de seguridad que sean pertinentes.

El valor puede ser propio, o puede ser acumulado. Se dice que los activos inferiores en un esquema de dependencias, acumulan el valor de los activos que se apoyan en ellos.

3. Dimensiones

De un activo puede interesar calibrar diferentes dimensiones:

a. **Su confidencialidad:** ¿qué daño causaría que lo conociera quien no debe? Esta valoración es típica de datos.

b. **Su integridad:** ¿qué perjuicio causaría que estuviera dañado o corrupto? Esta valoración es típica de los datos, que pueden estar manipulados, ser total o parcialmente falso o, incluso, faltar datos.

c. **Su disponibilidad:** ¿qué perjuicio causaría no tenerlo o no poder utilizarlo? Esta valoración es típica de los servicios.

d. **La autenticidad:** ¿qué perjuicio causaría no saber exactamente quien hace o ha hecho cada cosa?

e. **La trazabilidad del uso del servicio:** ¿qué daño causaría no saber a quién se le presta tal servicio? O sea, ¿quién hace qué y cuándo?

4. Valoración cualitativa

Las escalas cualitativas permiten avanzar con rapidez, posicionando el valor de cada activo en un orden relativo respecto de los demás. Es frecuente plantear estas escalas como “órdenes de magnitud” y, en consecuencia, derivar estimaciones del orden de magnitud del riesgo.

La limitación de las valoraciones cualitativas es que no permiten comparar valores más allá de su orden relativo. No se pueden sumar valores.

La ”Guía de Técnicas" presenta un modelo de análisis basado en valoraciones cualitativas.

5. Valoración cuantitativa

Las valoraciones numéricas absolutas cuestan mucho esfuerzo; pero permiten sumar valores numéricos de forma absolutamente “natural”. La interpretación de las sumas no es nunca motivo de controversia.

Si la valoración es dineraria, además se pueden hacer estudios económicos comparando lo que se arriesga con lo que cuesta la solución respondiendo a las preguntas:

¿Vale la pena invertir tanto dinero en esta salvaguarda?

¿Qué conjunto de salvaguardas optimizan la inversión?

La “Guía de Técnicas” presenta un modelo de análisis basado en valoraciones cuantitativas.

6. Criterios de valoración

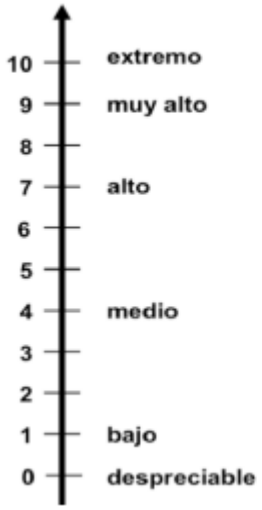
Para valorar los activos vale, teóricamente, cualquier escala de valores. A efectos prácticos sin embargo es muy importante.

Se usa una escala común para todas las dimensiones, permitiendo comparar riesgos. Se use una escala logarítmica, centrada en diferencias relativas de valor, que no en diferencias absolutas.

Se use un criterio homogéneo que permita comparar análisis realizados por separado.

Si la valoración es económica, hay poco más que hablar: dinero. Pero frecuentemente la valoración es cualitativa, quedando a discreción del usuario; es decir, respondiendo a criterios subjetivos.

Se ha elegido una escala detallada de diez valores, dejando en valor 0 como determinante de lo que sería un valor despreciable (a efectos de riesgo). Si se realiza un análisis de riesgos de poco detalle, se puede optar por la tabla simplificada de menos niveles. Ambas escalas, detallada y simplificada se correlacionan como se indica a continuación:



valor		*criterio*
10	extremo	daño extremadamente grave
9	muy alto	daño muy grave
6-8	alto	daño grave
3-5	medio	daño importante
1-2	bajo	daño menor
0	despreciable	irrelevante a efectos prácticos

Figura 3: Escala Detallada De Los Criterios De Evaluación

Fuente: (MAGERIT -- version 3.0.Libro Libro I:Metodo publicas, Gobierno de España-Ministerio De Hacienda y Relaciones, 2012)

7. El valor de la interrupción del servicio

Casi todas las dimensiones mencionadas anteriormente permiten una valoración simple, cualitativa o cuantitativa. Pero hay una excepción, la disponibilidad.

No es lo mismo interrumpir un servicio una hora o un día o un mes. Puede que una hora de detención sea irrelevante, mientras que un día sin servicio causa un daño moderado; pero un mes detenido suponga la terminación de la actividad. Y lo malo es que no existe proporcionalidad entre el tiempo de interrupción y las consecuencias.

2. D.1.2. Paso 2: Amenazas

El siguiente paso consiste en determinar las amenazas que pueden afectar a cada activo. Las amenazas son “cosas que ocurren”. Y, de todo lo que puede ocurrir, interesa lo que puede pasarle a nuestros activos y causar un daño.

1. **Identificación de las amenazas**

El capítulo 5 del "Catálogo de Elementos" presenta una relación de amenazas típicas. De Origen natural.

2. **Hay accidentes naturales (terremotos, inundaciones).**

Ante esos avatares el sistema de información es víctima pasiva, pero de todas formas tendremos en cuenta lo que puede suceder.

3. **Del entorno (de Origen industrial)**

Hay desastres industriales (contaminación, fallos eléctricos) ante los cuales el sistema de información es víctima pasiva; pero no por ser pasivos hay que permanecer indefensos.

4. **Defectos de las aplicaciones**

Hay problemas que nacen directamente en el equipamiento propio por defectos en su diseño o en su implementación, con consecuencias potencialmente negativas sobre el sistema. Frecuentemente se denominan vulnerabilidades técnicas o, simplemente, 'vulnerabilidades'

5. **Causadas por las personas de forma accidental**

Las personas con acceso al sistema de información pueden ser causa de problemas no intencionados, típicamente por error o por omisión.

6. **Causadas por las personas de forma deliberada**

Las personas con acceso al sistema de información pueden ser causa de problemas intencionados: ataques deliberados; bien con ánimo de beneficiarse indebidamente, bien con ánimo de causar daños y perjuicios a los legítimos propietarios.

No todas las amenazas afectan a todos los activos, sino que hay una cierta relación entre el tipo de activo y lo que le podría ocurrir.

7. **Valoración de las amenazas**

Cuando un activo es víctima de una amenaza, no se ve afectado en todas sus dimensiones, ni en la misma cuantía.

Una vez determinado que una amenaza puede perjudicar a un activo, hay que valorar su influencia en el valor del activo, en dos sentidos: Degradación: cuán perjudicado resultaría el [valor del] activo

Probabilidad: cuán probable o improbable es que se materialice la amenaza

La degradación mide el daño causado por un incidente en el supuesto de que ocurriera.

La degradación se suele caracterizar Como una fracción del valor del activo y así aparecen expresiones como que un activo se ha visto “totalmente degradado”, o “degradado en una pequeña fracción”. Cuando las amenazas no son intencionales, probablemente baste conocer la fracción físicamente perjudicada de un activo para calcular la pérdida proporcional de valor que se pierde. Pero cuando la amenaza es intencional, no se puede pensar en proporcionalidad alguna pues el atacante puede causar muchísimo daño de forma selectiva.

La probabilidad de ocurrencia es más compleja de determinar y de expresar. A veces se modela cualitativamente por medio de alguna escala nominal:

TABLA 1: Degradación Del Valor

MA	Muy alta	Casi seguro	Fácil
A	Alta	Muy alto	Medio
M	Media	Posible	Difícil
B	Baja	Poco probable	Muy difícil
MB	Muy baja	Muy raro	Extremadamente difícil

Fuente: (MAGERIT -- version 3.0.Libro Libro I:Metodo publicas, Gobierno de España-Ministerio De Hacienda y Relaciones, 2012)

A veces se modela numéricamente como una frecuencia de ocurrencia. Es habitual usar 1 año como referencia, de forma que se recurre a la tasa anual de ocurrencia como medida de la probabilidad de que algo ocurra. Son valores típicos:

TABLA 2: Probabilidad De Ocurrencia

MA	100	Muy frecuente	A diario
A	10	Frecuente	Mensualmente
M	1	Normal	Una vez al año
B	1/10	Poco frecuente	Cada varias años
MB	1/100	Muy poco frecuente	Siglos

Fuente: (MAGERIT -- version 3.0.Libro Libro I:Metodo publicas, Gobierno de España-Ministerio De Hacienda y Relaciones, 2012)

2.2.18. D.1.3. Determinación Del Impacto **Potencial**

Se denomina impacto a la medida del daño sobre el activo derivado de la materialización de una amenaza. Conociendo el valor de los activos (en varias dimensiones) y la degradación que causan las amenazas, es directo derivar el impacto que estas tendrían sobre el sistema.

La única consideración que queda hacer es relativa a las dependencias entre activos. Es frecuente que el valor del sistema se centre en la información que maneja y los servicios que presta; pero las amenazas suelen materializarse en los medios. Para enlazar unos con otros recurriremos al grafo de dependencias.

1. **Impacto Acumulado**

Es el calculado sobre un activo teniendo en cuenta

Su valor acumulado (el propio mas el acumulado de los activos que dependen de él)

Las amenazas a que está expuesto

El impacto acumulado se calcula para cada activo, por cada amenaza y en cada dimensión de valoración, siendo una función del valor acumulado y de la degradación causada.

El impacto es tanto mayor cuanto mayor es el valor propio o acumulado sobre un activo.

El impacto es tanto mayor cuanto mayor sea la degradación del activo atacado.

El impacto acumulado, al calcularse sobre los activos que soportan el peso del sistema de información, permite determinar las salvaguardas de que hay que dotar a los medios de trabajo: protección de los equipos, copias de respaldo, etc

2. Impacto Repercutido

Es el calculado sobre un activo teniendo en cuenta

Su valor propio

Las amenazas a que están expuestos los activos de los que depende

El impacto repercutido se calcula para cada activo, por cada amenaza y en cada dimensión de valoración, siendo una función del valor propio y de la degradación causada.

El impacto es tanto mayor cuanto mayor es el valor propio de un activo.

El impacto es tanto mayor cuanto mayor sea la degradación del activo atacado. El impacto es tanto mayor cuanto mayor sea la dependencia del activo atacado.

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

3. Agregación de valores de Impacto

Los párrafos anteriores determinan el impacto que sobre un activo tendría una amenaza en una cierta dimensión. Estos impactos singulares pueden agregarse bajo ciertas condiciones:

Puede agregarse el impacto repercutido sobre diferentes activos,

Puede agregarse el impacto acumulado sobre activos que no sean dependientes entre sí, no hereden valor de un activo superior común.

No debe agregarse el impacto acumulado sobre activos que no sean independientes, pues ello supondría sobre ponderar el impacto al incluir varias veces el valor acumulado de activos superiores,

Puede agregarse el impacto de diferentes amenazas sobre un mismo activo, aunque con-viene considerar en qué medida las diferentes amenazas son independientes y pueden ser concurrentes,

Puede agregarse el impacto de una amenaza en diferentes dimensiones.

2.2.19. D.1.4. Determinación del Riesgo Potencial

Se denomina riesgo a la medida del daño probable sobre un sistema. Conociendo el impacto de las amenazas sobre los activos, es directo derivar el riesgo sin más que tener en cuenta la probabilidad de ocurrencia. El riesgo crece con el impacto y con la probabilidad, pudiendo distinguirse una serie de zonas a tener en cuenta en el tratamiento del riesgo (que veremos más adelante):

Zona 1 — riesgos muy probables y de muy alto impacto

Zona 2 — franja amarilla: cubre un amplio rango desde situaciones improbables y de impacto medio, hasta situaciones muy probables pero de impacto bajo o muy bajo.

Zona 3 — riesgos improbables y de bajo impacto. Zona 4 — riesgos improbables pero de muy alto impacto

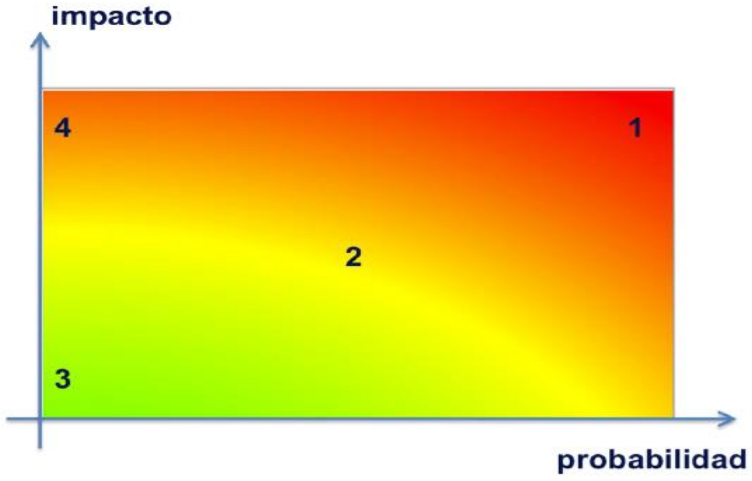


Figura 4: El Riesgo En Función DEL Impacto y La Probabilidad

Fuente: (MAGERIT -- version 3.0.Libro Libro I:Metodo publicas, Gobierno de España-Ministerio De Hacienda y Relaciones, 2012)

1. **Riesgo Acumulado**

Es el calculado sobre un activo teniendo en cuenta

El impacto acumulado sobre un activo debido a una amenaza.

La probabilidad de la amenaza

El riesgo acumulado se calcula para cada activo, por cada amenaza y en cada dimensión de valoración, siendo una función del valor acumulado, la degradación causada y la probabilidad de la amenaza.

El riesgo acumulado, al calcularse sobre los activos que soportan el peso Del Sistema de información, permite determinar las salvaguardas de que hay que dotar a los medios de trabajo: protección de los equipos, copias de respaldo, etc.

2. **Riesgo Repercutido**

Es el calculado sobre un activo teniendo en cuenta

El impacto repercutido sobre un activo debido a una amenaza.

La probabilidad de la amenaza

El riesgo repercutido se calcula para cada activo, por cada amenaza y en cada dimensión de valoración, siendo una función Del valor propio, la degradación causada y la probabilidad de la amenaza.

El riesgo repercutido, al calcularse sobre los activos que tienen valor propio, permite determinar las consecuencias de las incidencias técnicas sobre la misión del sistema de información. Es pues una presentación gerencial que ayuda a tomar una de las decisiones críticas de un análisis de riesgos: aceptar un cierto nivel de riesgo.

3. **Agregación de Riesgos**

Los párrafos anteriores determinan el riesgo que sobre un activo tendría una amenaza en una cierta dimensión. Estos riesgos singulares pueden agregarse bajo ciertas condiciones:

Puede agregarse el riesgo repercutido sobre diferentes activos.

Puede agregarse el impacto acumulado sobre activos que no sean dependientes entre sí, y no hereden valor de un activo superior común.

No debe agregarse el riesgo acumulado sobre activos que no sean independientes, pues ello supondría sobre ponderar el riesgo al incluir varias veces el valor acumulado de activos superiores.

Puede agregarse el riesgo de diferentes amenazas sobre un mismo activo, aunque conviene considerar en qué medida las diferentes amenazas son independientes y pueden ser concurrentes.

Puede agregarse el riesgo de una amenaza en diferentes dimensiones.

4. D.1.5. Paso 3: Salvaguardas

En los pasos anteriores no se han tomado en consideración las salvaguardas desplegadas. Se miden, por tanto, los impactos y riesgos a que estarían expuestos los activos si no se protegieran en absoluto. En la práctica no es frecuente encontrar sistemas desprotegidos: las medidas citadas indican lo que ocurriría si se retiraran las salvaguardas presentes. Se definen las salvaguardas o contra medidas Como aquellos procedimientos o mecanismos tecnológicos que reducen el riesgo. Hay amenazas que se conjurar simplemente organizándose adecuadamente, otras requieres elementos técnicos (programas o equipos), otra seguridad física y, por último, está la política de personal. El capítulo 6 Del "Catálogo de Elementos" presenta una relación de salvaguardas adecuadas para cada tipo de activos.

1. **Selección de Salvaguardas**

   Ante el amplio abanico de posibles salvaguardas a considerar, es necesario hacer una criba inicial para quedarnos con aquellas que son

relevantes para lo que hay que proteger. En esta criba se deben tener en cuenta los siguientes aspectos:

Tipo de activos a proteger, pues cada tipo se protege de una forma específica

Dimensión o dimensiones de seguridad que requieren protección

Amenazas de las que necesitamos protegernos

Si existen salvaguardas alternativas

Además, es prudente establecer un principio de proporcionalidad y tener en cuenta:

El mayor o menor valor propio o acumulado sobre un activo, centrándonos en lo más valioso y obviando lo irrelevante.

La mayor o menor probabilidad de que una amenaza ocurra, centrándonos en los riesgos más importantes (ver zonas de riesgo).

La cobertura del riesgo que proporcionan salvaguardas alternativas.

Esto lleva a dos tipos de declaraciones para excluir una cierta salvaguarda del conjunto de las que conviene analizar:

No aplica — se dice cuando una salvaguarda no es de aplicación porque técnicamente no es adecuada al tipo de activos a proteger, no protege la dimensión necesaria o no protege frente a la amenaza en consideración

No se justifica — se dice cuando la salvaguarda aplica, pero es desproporcionada al riesgo que tenemos que proteger.

Como resultado de estas consideraciones dispondremos de una “declaración de aplicabilidad” o relación de salvaguardas que deben ser analizadas como componentes nuestro sistema de protección.

a. Efecto de las Salvaguardas

Las salvaguardas entran en el cálculo del riesgo de dos formas:

b. Reduciendo la probabilidad de las amenazas

Se llaman salvaguardas preventivas. Las ideales llegan a impedir completamente que la amenaza se materialice.

c. Limitando el daño causado

Hay salvaguardas que directamente limitan la posible degradación, mientras que otras permiten detectar inmediatamente el ataque para frenar que la degradación avance. Incluso algunas salvaguardas se limitan a permitir la pronta recuperación del sistema cuando la amenaza lo destruye. En cualquiera de las versiones, la amenaza se materializa; pero las con-secuencias se limitan.

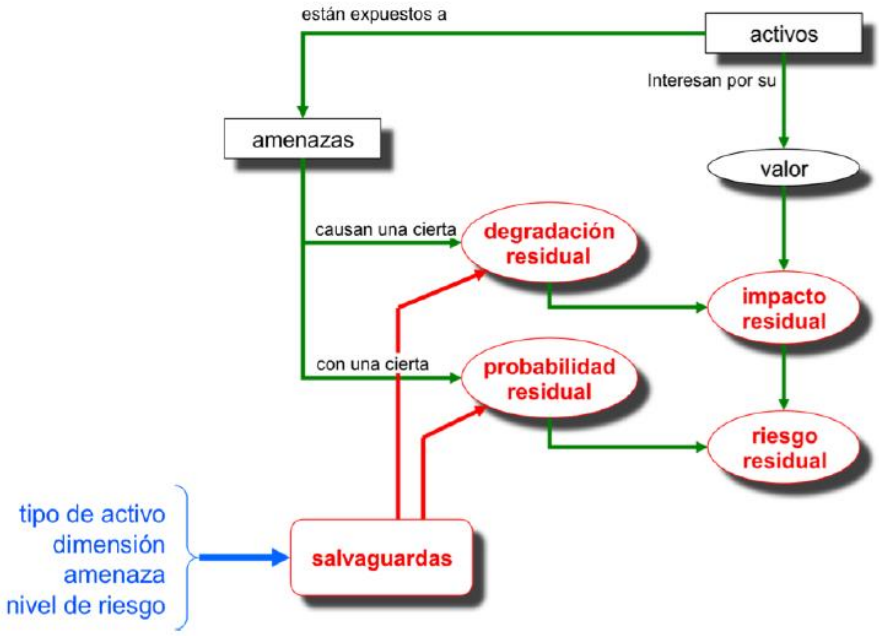


Figura 5: Elementos De Análisis Del Riesgo Residual

Fuente: (MAGERIT -- version 3.0.Libro Libro I:Metodo publicas, Gobierno de España-Ministerio De Hacienda y Relaciones, 2012)

d. Tipo de Protección

Esta aproximación a veces resulta un poco simplificadora, pues es habitual hablar de diferentes tipos de protección prestados por las salvaguardas:

[PR] Prevención

Diremos que una salvaguarda es preventiva cuando reduce las oportunidades de que un incidente ocurra. Si la salvaguarda falla y el incidente llega a ocurrir, los daños son los mismos. Ejemplos: autorización previa de los usuarios, gestión de

privilegios, planificación de capacidades, metodología Segura de desarrollo de software, pruebas en pre-producción, segregación de tareas.

[DR] Disuasión

Diremos que una salvaguarda es disuasoria cuando tiene un efecto tal sobre los atacantes que estos no se atreven o se lo piensan dos veces antes de atacar. Son salvaguardas que actúan antes del incidente, reduciendo las probabilidades de que ocurra; pero que no tienen influencia sobre los daños causados caso de que el atacante realmente se atreva. Ejemplos: vallas elevadas, guardias de seguridad, avisos sobre la persecución del delito o persecución del delincuente.

[EL] Eliminación

Diremos que una salvaguarda elimina un incidente cuando impide que éste tenga lugar. Son salvaguardas que actúan antes de que el incidente se haya producido. No reducen los daños caso de que la salvaguarda no sea perfecta y el incidente llegue a ocurrir.

Ejemplos: eliminación de cuentas estándar, de cuentas sin contraseña, de servicios innecesarios; en general, todo lo que tenga que ver con la fortificación o bastionado, cifrado de la información, armarios ignífugos.

[IM] Minimización del impacto / Limitación del impacto

Se dice que una salvaguarda minimiza o limita el impacto cuando acota las consecuencias de un incidente. Ejemplos: desconexión de redes o equipos en caso de ataque, detención de servicios en caso de ataque, seguros de cobertura, cumplimiento de la legislación vigente.

[CR] Corrección

Diremos que una salvaguarda es correctiva cuando, habiéndose producido un daño, lo repara. Son salvaguardas que actúan después de que el incidente se haya producido y por tanto reducen los daños.

Véase: recuperación más abajo. Ejemplos: gestión de incidentes, líneas de comunicación alternativas, Fuentes de alimentación redundantes.

[RC] Recuperación

Diremos que una salvaguarda ofrece recuperación cuando permite regresar al estado anterior al incidente. Son salvaguardas que no reducen las probabilidades del incidente, pero acotan los daños a un periodo de tiempo.

Ejemplos: copias de seguridad (back-up).

[MN] Monitorización

Son las salvaguardas que trabajan monitorizando lo que está ocurriendo o lo que ha ocurrido. Si se detectan cosas en tiempo real, podemos reaccionar atajando el incidente para limitar el impacto; si se detectan cosas a posterior, podemos aprender del incidente y mejorar el sistema de salvaguardas de cara al futuro. Ejemplos: registros de actividad, registro de descargas de web.

[DC] Detección

Diremos que una salvaguarda funciona detectando un ataque cuando informa de que el ataque está ocurriendo. Aunque no impide el ataque, sf permite que entren en operación otras medidas que atajen la progresión del ataque, minimizando daños. Ejemplos: anti-virus, lDS, detectores de incendio.

[AW] Concienciación

Son las actividades de formación de las personas anexas al sistema que pueden tener una influencia sobre él. La formación reduce los errores de los usuarios, lo cual tiene un efecto preventivo. También mejora las salvaguardas de todo tipo pues los que las operan lo hacen con eficacia y rapidez, potenciando su efecto o, al menos, no menoscabándolo por una mala operación. Ejemplos: cursos de concienciación, cursos de formación.

[AD] Administración

Se refiere a las salvaguardas relacionadas con los componentes de seguridad del sistema. Una buena administración evita el desconocimiento de lo que hay y por tanto impide que haya puertas desconocidas por las que pudiera tener éxito un ataque. En general pueden considerarse medidas de tipo preventivo.

Ejemplos: inventario de activos, análisis de riesgos, plan de continuidad. La siguiente tabla relaciona cada uno de estos tipos de protección con el modelo anterior de reducción de la degradación y de la probabilidad:

efecto	tipo
preventivas: reducen la probabilidad	[PR] preventivas [DR] disuasorias [EL] eliminatorias
acotan la degradación	[IM] minimizadoras [CR] correctivas [RC] recuperativas
consolidan el efecto de las demás	[MN] de monitorización [DC] de detección [AW] de concienciación [AD] administrativas

Figura 6: Tipos De Salvaguardas

Fuente: (MAGERIT -- version 3.0.Libro Libro I:Metodo publicas, Gobierno de España-Ministerio De Hacienda y Relaciones, 2012)

e. Eficacia de la protección

Las salvaguardas se caracterizan, además de por su existencia, por su eficacia frente al riesgo que pretenden conjurar. La salvaguarda ideal es 100% eficaz, eficacia que combina 2 factores:

Desde el punto de vista técnico

Es técnicamente idónea para enfrentarse al riesgo que protege se emplea siempre

Desde el punto de vista de operación de la salvaguarda

Está perfectamente desplegada, configurada y mantenida

Existen procedimientos claros de uso normal y en caso de incidencias

Los usuarios están formados y concienciados existen controles que avisan de posibles fallos

Entre una eficacia del 0% para aquellas que faltan y el 100% para aquellas que son idóneas y que están perfectamente implantadas, se estimará un grado de eficacia real en cada caso concreto. Para medir los aspectos organizativos, se puede emplear una escala de madurez que recoja en forma de factor corrector la confianza que merece el proceso de gestión de la salvaguarda:

factor	nivel	significado
0%	**L0**	inexistente
	L1	inicial / ad hoc
	L2	reproducible, pero intuitivo
	L3	proceso definido
	L4	gestionado y medible
100%	**L5**	optimizado

Figura 7: Eficacia y madurez de las salvaguardas

Fuente: (MAGERIT -- version 3.0.Libro Libro I:Metodo publicas, Gobierno de España-Ministerio De Hacienda y Relaciones, 2012)

f. Vulnerabilidades

Se denomina vulnerabilidad a toda debilidad que puede ser aprovechada por una amenaza, o más detalladamente a las debilidades de los activos o de sus medidas de protección que facilitan el éxito de una amenaza potencial.

Traducido a los términos empleados en los párrafos anteriores, son vulnerabilidades todas las ausencias o ineficacias de las salvaguardas pertinentes para salvaguardar el valor propio o acumulado sobre un activo. A veces se emplea el término “insuficiencia” para resaltar el hecho de que la eficacia medida de la salvaguarda es insuficiente para preservar el valor del activo expuesto a una amenaza.

5. D.1.5. Paso 4: Impacto Residual

Dado un cierto conjunto de salvaguardas desplegadas y una medida de la madurez de su proceso de gestión, el sistema queda en una situación de posible impacto

que se denomina residual. Se dice que hemos modificado el impacto, desde un valor potencial a un valor residual.

El cálculo del impacto residual es sencillo. Como no han cambiado los activos, ni sus dependencias, sino solamente la magnitud de la degradación, se repiten los cálculos de impacto con este nuevo nivel de degradación.

La magnitud de la degradación tomando en cuenta la eficacia de las salvaguardas, es la proporción que resta entre la eficacia perfecta y la eficacia real.

El impacto residual puede calcularse acumulado sobre los activos inferiores, o repercutido sobre los activos superiores.

2.2.20. D.1.5. Paso 5: Riesgo Residual

Dado un cierto conjunto de salvaguardas desplegadas y una medida de la madurez de su proceso de gestión, el sistema queda en una situación de riesgo que se denomina residual. Se dice que hemos modificado el riesgo, desde un valor potencial a un valor residual. El cálculo del riesgo residual es sencillo. Como no han cambiado los activos, ni sus dependencias, sino solamente la magnitud de la degradación y la probabilidad de las amenazas, se repiten los cálculos de riesgo usando el impacto residual y la probabilidad residual de ocurrencia.

La magnitud de la degradación se toma en consideración en el cálculo del impacto residual. La magnitud de la probabilidad residual tomando en cuenta la eficacia de las salvaguardas, es la proporción que resta entre la eficacia perfecta y la eficacia real. El riesgo residual puede calcularse acumulado sobre los activos inferiores, o repercutido sobre los activos superiores.

1. **Documentación**

Documentación intermedia

Resultados de las entrevistas.

Documentación de otras Fuentes: estadísticas, observaciones de expertos y observaciones de los analistas.

Información existente utilizable por el proyecto.

Documentación auxiliar: planos, organigramas, requisitos, especificaciones, análisis funcionales, cuadernos de carga, manuales de usuario, manuales de explotación, diagramas de flujo de información y de procesos, modelos de datos, etc.

Informes y evaluaciones de defectos de los productos, procedentes de fabricantes o de centros de respuesta a incidentes de seguridad (CERTs).

Documentación final:

2. **Modelo de valor**

Informe que detalla los activos, sus dependencias, las dimensiones en las que son valiosos y la estimación de su valor en cada dimensión.

3. **Mapa de riesgos:**

Informe que detalla las amenazas significativas sobre cada activo, caracterizándolas por su frecuencia de ocurrencia y por la degradación que causaría su materialización sobre el activo.

4. **Declaración de aplicabilidad:**

Informe que recoge las contramedidas que se consideran apropiadas para defender el sistema de información bajo estudio.

5. **Evaluación de salvaguardas:**

Informe que detalla las salvaguardas existentes calificándolas en su eficacia para reducir el riesgo que afrontan.

6. **Informe de insuficiencias o vulnerabilidades:**

Informe que detalla las salvaguardas necesarias pero ausentes o insuficientemente eficaces.

7. **Estado de riesgo:**

Informe que detalla para cada activo el impacto y el riesgo, potenciales y residuales, frente a cada amenaza.

8. Proceso de Gestión de Riesgos

A la vista de los impactos y riesgos a que está expuesto el sistema, hay que tomar una serie de decisiones condicionadas por diversos factores:

La gravedad del impacto y/o del riesgo.

Las obligaciones a las que por Iey esté sometida la Organización.

Las obligaciones a las que por reglamentos sectoriales esté sometida la Organización.

Las obligaciones a las que por contrato esté sometida la Organización.

Dentro del margen de maniobra que permita este marco, pueden aparecer consideraciones adicionales sobre la capacidad de la Organización para aceptar ciertos impactos de naturaleza intangible tales como:

Imagen pública de cara a la Sociedad (aspectos reputaciones)

Política interna: relaciones con los propios empleados, tales como capacidad de contratar al personal idóneo, capacidad de retener a los mejores, capacidad de soportar rotaciones de personas, capacidad de ofrecer una carrera profesional atractiva, etc.

Relaciones con los proveedores, tales como capacidad de llegar a acuerdos ventajosos a corto, medio o largo plazo, capacidad de obtener trato prioritario, etc.

Relaciones con los clientes o usuarios, tales como capacidad de retención, capacidad de incrementar la oferta, capacidad de diferenciarse frente a la competencia.

Relaciones con otras organizaciones, tales como capacidad de alcanzar Acuerdos estratégicos, alianzas, etc.

Nuevas oportunidades de negocio, tales como formas de recuperar la inversión en seguridad

Acceso a sellos o calificaciones reconocidas de seguridad

Todas las consideraciones anteriores desembocan en una calificación de cada riesgo significativo, determinándose sí.

1. Es crítico en el sentido de que requiere atención urgente.
2. Es grave en el sentido de que requiere atención.
3. Es apreciable en el sentido de que pueda ser objeto de estudio para su tratamiento.
4. Es asumible en el sentido de que no se van a tomar acciones para atajarlo.

La opción 4, aceptación del riesgo, siempre es arriesgada y hay que tomarla con prudencia y justificación. Las razones que pueden llevar a esta aceptación son:

a. Cuando el impacto residual es asumible.
b. Cuando el riesgo residual es asumible.
c. Cuando el coste de las salvaguardas oportunas es desproporcionado en comparación al impacto y riesgo residuales.

La calificación de los riesgos tendrá consecuencias en las tareas subsiguientes, siendo un factor básico para establecer la prioridad relativa de las diferentes actuaciones.

El análisis de riesgos determina impactos y riesgos. Los impactos recogen daños absolutos, independientemente de que sea más o menos probable que se dé la circunstancia. En cambio, el riesgo pondera la probabilidad de que ocurra. El impacto refleja el daño posible (lo peor que puede ocurrir), mientras que el riesgo refleja el daño probable (lo que probablemente ocurra). El resultado Del análisis es sólo UN análisis. A partir de el disponemos de información para tomar decisiones conociendo lo que queremos proteger (activos valorados=, de qué lo queremos proteger (amenazas valoradas) y qué hemos hecho por protegerlo (salvaguardas valoradas). Todo ello sintetizado en los valores de impacto y riesgo. A partir de aquí, las decisiones son de los órganos de gobierno de la Organización que actuarán en 2 pasos:

Paso 1: Evaluación

Paso 2: Tratamiento

El siguiente grafico resume las posibles decisiones que se pueden tomar tras Haber estudiado los riesgos. La caja 'estudio de los riesgos' pretende combinar el análisis con la evaluación.

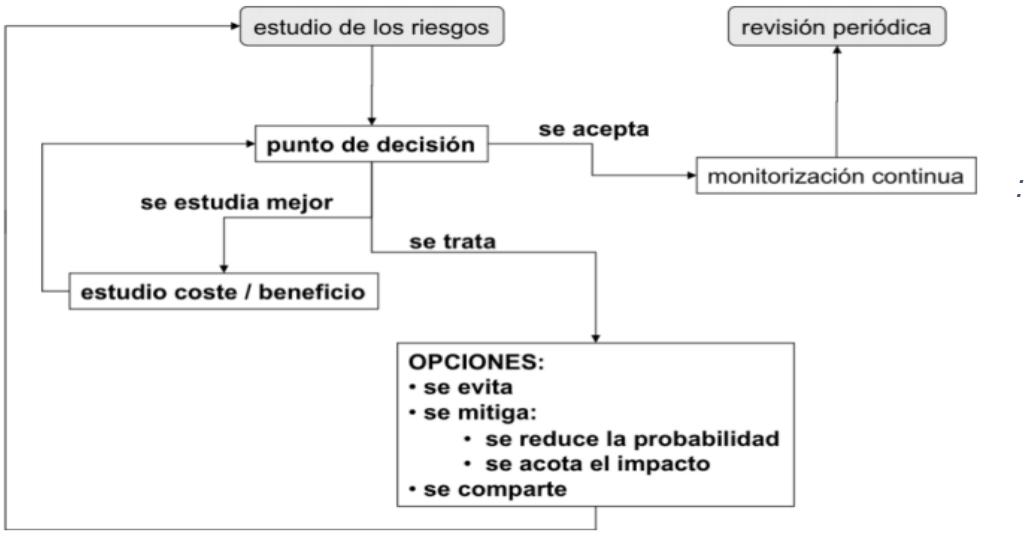


Figura 8: Decisiones de tratamiento de los riesgos

Fuente: (MAGERIT -- version 3.0.Libro Libro I:Metodo publicas, Gobierno de España-Ministerio De Hacienda y Relaciones, 2012)

9. **Evaluación:** Interpretación de los valores de impacto y riesgo residuales Impacto y riesgo residual son una medida del estado presente, entre la inseguridad potencial (sin salvaguarda alguna) y las medidas adecuadas que reducen impacto y riesgo a valores aceptables. Los párrafos siguientes se refieren conjuntamente a impacto y riesgo. Si el valor residual es igual al valor potencial, las salvaguardas existentes no valen para nada, típicamente no porque no haya nada hecho, sino porque hay elementos fundamentales sin hacer. Es importante entender que un valor residual es sólo un número. Para su correcta interpretación debe venir acompañado de la relación de lo que se debería hacer y no se ha hecho; es decir, de las vulnerabilidades que presenta el sistema. Los responsables de la toma de decisiones deberán prestar cuidadosa

atención a esta relación de tareas pendientes, que se denomina Informe de insuficiencias o de vulnerabilidades.

10. Aceptación del riesgo

La Dirección de la Organización sometida al análisis de riesgos debe determinar el nivel de impacto y riesgo aceptable. Más propiamente dicho, debe aceptar la responsabilidad de las insuficiencias. Esta decisión no es técnica. Puede ser una decisión política o gerencial o puede venir determinada por ley o por compromisos contractuales con proveedores o usuarios. Estos niveles de aceptación se pueden establecer por activo o por agregación de activos (en un determinado departamento, en un determinado servicio, en una determinada dimensión.)

11. Tratamiento

La Dirección puede decidir aplicar algún tratamiento al sistema de seguridad desplegado para proteger el sistema de información. Hay dos grandes opciones:

Reducir el riesgo residual (aceptar un menor riesgo).

Ampliar el riesgo residual (aceptar un mayor riesgo).

Para tomar una u otra decisión hay que enmarcar los riesgos soportados por el sistema de información dentro de un contexto más amplio que cubre un amplio espectro de consideraciones de las que podemos apuntar algunas sin pretender ser exhaustivos:

Cumplimiento de obligaciones; sean legales, regulación pública o sectorial, compromisos in-ternos, misión de la Organización, responsabilidad corporativa, etc.

Posibles beneficios derivados de una actividad que en sí entraña riesgos Condicionantes técnicos, económicos, culturales, políticos, etc.

Equilibrio con otros tipos de riesgos: comerciales, financieros, regulatorios, medioambientales, laborales, En condiciones de riesgo residual extremo, casi la única opción es reducir el riesgo. En condiciones de riesgo residual aceptable, podemos optar entre aceptar el nivel actual o ampliar el riesgo asumido. En

cualquier caso hay que mantener unamonitorización continua de las circunstancias para que el riesgo formal cuadre con la experiencia real y reaccionemos ante cualquier desviación significativa.

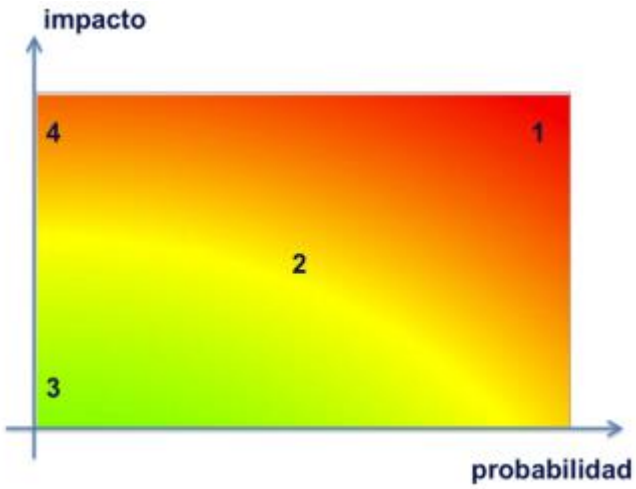


Figura 9: Zonas De Riesgo

Fuente: MAGERIT — versión 3.0. Libro I: Método. Gobierno de España — Ministerio De Hacienda Y Relaciones Públicas. 2012

A. Opciones de Tratamiento del Riesgo: Eliminación

La eliminación de la fuente de riesgo es una opción frente a un riesgo que no es aceptable. En un sistema podemos eliminar varias cosas, siempre que no afecten a la esencia de la Organización. Es extremadamente raro que podamos prescindir de la información o los servicios esenciales por cuanto constituyen la misión de la Organización. Cambiar estos activos supone reorientar la misión de la Organización.

Más viable es prescindir de otros componentes no esenciales, que están presentes simple y llanamente para implementar la misión, pero no son parte constituyente de la misma. Esta opción puede tomar diferentes formas:

Eliminar cierto tipo de activos, emplean otros en su lugar. Por ejemplo: cambiar de sistema operativo, de fabricante de equipos,...

Reordenar la arquitectura del sistema (el esquema de dependencias en nuestra terminología) de forma que alteremos el valor acumulado en ciertos activos expuestos a grandes amenazas. Por ejemplo: segregar redes, desdoblar equipos para atender a necesidades concretas, alejando lo más valioso de lo más expuesto.

Las decisiones de eliminación de las fuentes de riesgo suponen realizar un nuevo análisis de riesgos sobre el sistema modificado.

B. Opciones de Tratamiento del Riesgo: Mitigación

La mitigación del riesgo se refiere a una de dos opciones:

Reducir la degradación causada por una amenaza (a veces se usa la expresión acotar el impacto')

Reducir la probabilidad de que una amenaza de materializa

En ambos casos lo que hay que hacer es ampliar o mejorar el conjunto de salvaguardas. En términos de madurez de las salvaguardas: subir de nivel.

C. Opciones de Tratamiento del Riesgo: Compartición

Tradicionalmente se ha hablado de 'transferir el riesgo'. Como la transferencia puede ser parcial o total, es más general hablar de 'compartir el riesgo'. Hay dos formas básicas de compartir riesgo:

1. **Riesgo cualitativo:**

   Se comparte por medio de la externalización de componentes del sistema, de forma que se reparten responsabilidades: unas técnicas para el que opera el componen-te técnico; y otras legales según el acuerdo que se establezca de prestación del servicio.

2. **Riesgo cuantitativo:**

   Se comparte por medio de la contratación de seguros, de forma que a cambio de una prima, el tomador reduce el impacto de las posibles amenazas y el asegurador corre con las consecuencias. Hay multitud de tipos y cláusulas de seguros para concretar el grado de

responsabilidad de cada una de las partes. Cuando se comparten riesgos cambia, bien el conjunto de componentes del sistema, bien su valoración, requiriéndose un nuevo análisis del sistema resultante.

D. Opciones de Tratamiento del Riesgo: Financiación

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

E. Documentación de proceso Documentación interna

1. Definición de roles, funciones y esquemas de reporte
2. Criterios de valoración de la información
3. Criterios de valoración de los servicios
4. Criterios de evaluación de los escenarios de impacto y riesgo Documentación para otros.
5. Plan de Seguridad

F. Plan de seguridad

Esta sección trata de cómo llevar a cabo planes de seguridad, entendiendo por tales proyectos para materializar las decisiones adoptadas para el tratamiento de los riesgos.

Estos planes reciben diferentes nombres en diferentes contextos y circunstancias:

a. Plan de mejora de la seguridad
b. Plan director de seguridad
c. Plan estratégico de seguridad
d. Plan de adecuación (en concreto es el nombre que se usa en el ENS)

2.2.21. **Herramienta Pilar (7.1.9 - 31.5.2018).**

Procedimiento Informático Lógico de Análisis de Riesgos, PILAR, es una aplicación implementada en java basada en la metodología MAGERIT, desarrollada por el Centro Cristológico Nacional y con un gran calado en la administración pública española. La versión vigente es la (7.1.9 - 31.5.2018).. Su licencia de prueba es de 30 días, no obstante para uso en entorno privado dicha licencia tiene un coste.

La herramienta permite la realización de análisis de riesgos bajo un enfoque tanto cualitativo como cuantitativo (empleando valores simbólicos o económicos respectivamente) y la realización de análisis de impacto en el ámbito de la continuidad de negocio.

Figura 10: Diagrama De Los Proceso De Análisis y Gestión De Riesgos
Fuente: (MAGERIT -- version 3.0.Libro Libro I:Metodo publicas, Gobierno de España-Ministerio De Hacienda y Relaciones, 2012)

2.2.22. **Análisis y Gestión de riesgos**

Se analizan los riesgos en varias dimensiones:

1. Confidencialidad
2. Integridad

3. Disponibilidad
4. Autenticidad
5. Trazabilidad

Para tratar el riesgo se proponen:

Salvaguardas (o contramedidas)

Normas de seguridad

Procedimientos de seguridad

Analizándose el riesgo residual a lo largo de diversas etapas de tratamiento

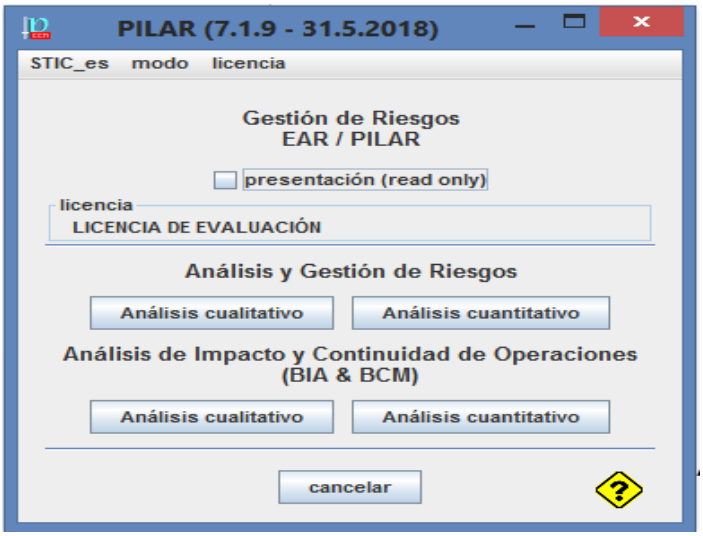


Figura 11: Herramienta Pilar - Pantalla de Principal

Fuente: Herramienta Pilar en su versión (7.1.9 - 31.5.2018).

2.2.23. **Criterios de Selección de la Metodología Magerit**

Para la elaboración del análisis y gestión de riesgos en los servidores, existen varias guías informales, aproximaciones metodológicas, estándares y herramientas de soporte que buscan gestionar y mitigar los riegos. Las principales metodologías de análisis y gestión de riesgos de uso habitual en el mercado de la seguridad de las tecnologías de la información son: MAGERIT, OCTAVE, CRAMM, IRAM, para

Determinar por qué MAGERIT es un buena elección para el desarrollo del AGR se presenta un cuadro comparativo.

TABLA 3: Comparativa de Metodologías de Análisis y Gestión de Riesgos

		MAGERIT	OCTAVE	CRAMM	IRAM
Alcance considerado	Análisis de riesgos	SI	SI	SI	SI
	Gestión de riesgos	SI	SI	SI	SI
Tipo de análisis	Cuantitativo	SI	NO	SI	SI
	Cualitativo	SI	NO	SI	SI
	Mixto	SI	NO	NO	NO

Fuente: Elaborada por el autor basado en estudios comparativos de la metodología teniendo cono principal fuente a la Tesis: Análisis De Riesgos De Seguridad Informática, Universidad Politécnica - Madrid.

MAGERIT es la metodología recomendada para el análisis y gestión de riesgos, el cual Permite realizar una evaluación profunda de la seguridad de los sistemas de información.

2.2.24. **Criterios de Selección de la Herramienta Pilar**

En la selección de la herramienta para el AGR, para el presente proyecto, se tomó en cuenta el análisis comparativo de las herramientas disponibles, como se observa en el cuadro siguiente.

TABLA 4: Análisis Comparativo De Las Herramientas AGR.

herramienta	Metodología	Idioma	Estándares
CRAMM	Evaluación de riesgos CRAMM	Inglés, holandés, checo	ISO 27001
TOOL KIT	----------	Inglés, portugués	ISO 27000
RISICARE	MEHARI	Francés, ingles	ISO 17799, ISO 27001
ORICO	OGRCM	Español, ingles	----------
PILAR	MAGERIT	Español, ingles	ISO 2701, ISO 1540, ISP 17999, ISO 1995

Fuente: Elaboración propia por el autor basado en estudios comparativos de la metodología teniendo cono principal fuente a la Tesis: Análisis De Riesgos De Seguridad Informática, Universidad Politécnica - Madrid.

Del análisis, se selecciona la herramienta PILAR, por los siguientes motivos:

Contiene los modelos de la madurez CMMI.

Se basa en Normas, estándares, código de buenas prácticas para la gestión de la seguridad.

Para la utilización de la herramienta PILAR, es necesario disponer de una licencia de USO, en el caso del presente proyecto se solicitó una licencia de evaluación de 30 días con el apoyo del asesor de tesis.

2.3. **Definición de téminos básicos:**

Auditoría Operativa: Está diseñada para evaluar la estructura de control interno en un área determinada

Auditoría Externa: Es aquella que es realizada por personas ajenas a la empresa auditada.

Auditoría Global: Es aquella que combina tanto pasos de auditoría contables como operativas.

Eficacia: Es aquello que permite que una cosa sea eficaz**.**

Eficiencia: Conjunto de atributos que se refieren a las relaciones entre el nivel de rendimiento del software y la cantidad de recursos utilizados bajo unas condiciones predefinidas.

Disponibilidad: Es aquello que se alcanza si las personas autorizadas pueden acceder a tiempo a la información a la que estén autorizadas.

Control de Calidad: Es aquello que asegura que las prestaciones son exactas y apropiadas sobre el servicio o producto.

Confidencialidad: Es aquello que se cumple cuando sólo las personas autorizadas pueden conocer los datos o la información correspondiente.

Auditoría Interna: Es aquella que es realizada con recursos materiales y personas que pertenecen a la Empresa auditada.

Evaluación de Riesgo: Es el proceso utilizado para identificar y evaluar riesgos y su impacto potencial.

Evidencia: Es toda información que utiliza el AI para determinar si el ente o los datos auditados siguen los criterios u objetivos de la auditoría.

Herramienta: Es el conjunto de elementos físicos utilizados para llevar a cabo las acciones y pasos definidos en la técnica

Herramienta de Control: Son elementos de software que permiten definir uno o varios procedimientos de control para cumplir una normativa y un objetivo de control.

Herramientas de software de auditoría: Son programas computarizados que pueden utilizarse para brindar información para uso de auditoría.

Programa de Auditoría: Es un conjunto documentado de procedimientos de auditoría diseñados para alcanzar los objetivos de auditoría planificados.

Documentación de Auditoría de SI: Es el registro del trabajo de auditoría realizado y la evidencia que respalda los hallazgos y conclusiones del auditor.

Controles Generales: Son controles interdependientes válidos para todas las áreas de la organización.

Riesgo: Es la posibilidad de que ocurra un hecho o suceso que pueda tener efecto adverso sobre la organización y sus sistemas de información.

Riesgo de control: Es el riesgo que los sistemas de control en vigencia no puedan detectar o evitar errores o irregularidades significativas en forma oportuna.

Riesgo de detección: Es el riesgo que a través de la labor de auditoría no se detecten errores o irregularidades significativas en el caso que existiesen y no hubiesen sido prevenidos o detectados por los sistemas de control

Vulnerabilidad: Es la situación creada, por falta de uno o varios controles, con lo que la amenaza pudiera crecer y así afectar al entorno informático (informatica, s.f.).

Activo: Componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con· consecuencias para la organización. Incluye: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos.

Amenaza: Causa potencial de un incidente que puede causar daños a un sistema de información o a una organización.

Análisis de riesgos: Proceso sistemático para estimar la magnitud de los riesgos a que está expuesta una Organización. Identificación de las amenazas que acechan a los distintos componentes pertenecientes o relacionados con el sistema de información (conocidos como 'activos');para determinar la vulnerabilidad del sistema ante esas amenazas y para estimar el impacto o grado de perjuicio que una seguridad insuficiente puede tener para la organización, obteniendo cierto conocimiento del riesgo que se corre.

Ataque: Intento de destruir, exponer, alterar o inhabilitar un sistema de información o la información que el sistema maneja, o violar alguna política de seguridad de alguna otra manera.

Auditoría de seguridad: Estudio y examen independiente del historial y actividades de un sistema de información, con la finalidad de comprobar la idoneidad de los controles del sistema, asegurar su conformidad con la estructura de seguridad y procedimientos operativos establecidos, a fin de detectar brechas en la seguridad y recomendar cambios en los procedimientos, controles y estructuras de seguridad.

Autenticidad: Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos. Contra la autenticidad de la información podemos tener manipulación del origen o el contenido de los datos. Contra la autenticidad de los usuarios de los servicios de acceso, podemos tener suplantación de identidad.

Confidencialidad: Que la información llegue solamente a las personas autorizadas. Contra la confidencialidad o secreto pueden darse fugas y filtraciones de información, así como accesos no autorizados.

Disponibilidad: Disposición de los servicios a ser usados cuando sea necesario. La carencia de disponibilidad supone una interrupción del servicio. La disponibilidad afecta directamente a la productividad de las organizaciones.

Estado de riesgo: Caracterización de los activos por su riesgo residual; es decir, por lo que puede pasar teniendo en cuenta las salvaguardas desplegadas.

Evaluación de salvaguardas: Evaluación de la eficacia de las salvaguardas existentes en relación al riesgo que afrontan.

Gestión de riesgos: Actividades coordinadas para dirigir y controlar una organización. Selección e implantación de salvaguardas para conocer, prevenir, impedir, reducir o controlar los riesgos identificados. Selección e implantación de las medidas o 'salvaguardas' de seguridad adecuadas para conocer, prevenir, impedir, reducir o controlar los riesgos identificados y así reducir al mínimo su potencialidad o sus posibles perjuicios. La gestión de riesgos se basa en los resultados obtenidos en el análisis de los riesgos.

Integridad: Mantenimiento de las características de completitud y corrección de los datos. Contra la integridad, la información puede aparecer manipulada, corrupta o incompleta. La integridad afecta directamente al correcto desempeño de las funciones de una Organización.

Mapa de riesgos: Relación de las amenazas a que están expuestos los activos.

Plan de seguridad: Conjunto de proyectos de seguridad que permiten materializar las decisiones de gestión de riesgos.

Riesgo: Estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la Organización. Efecto de la incertidumbre sobre la consecución de los objetivos

Salvaguarda: Procedimiento o mecanismo tecnológico que reduce el riesgo.

Seguridad: La capacidad de las redes o de los sistemas de información de resistir, con un determinado nivel de confianza, los accidentes o acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos y de los servicios que dichas redes y sistemas ofrecen o hacen accesibles .

Seguridad de la información: Confianza en que los sistemas de información están libres y exentos de todo peligro o daño inaceptables.

Trazabilidad: Aseguramiento de que en todo ·momento se podrá determinar quién hizo qué y en qué momento. La trazabilidad es esencial para analizar los incidentes, perseguir a los atacantes y aprender de la experiencia. La trazabilidad se materializa en la integridad de los registros de actividad.

2.4. **Hipótesis**

La presente investigación por ser de carácter descriptivo – propositiva, presenta una hipótesis implícita.

III. MATERIALES Y METODOS

3.1. **Variables y Operacionalización de Variables**

3.1.1. **Variable única.**

X: auditoria de seguridad para vulnerabilidades de la red informática de la Universidad Señor de Sipan.

3.1.2. **Operacionalización**

Variable	Dimensión	Indicador	Ítems	Instrumento
Auditoria de seguridad para vulnerabilidades de la red informática	Autentificación de Usuarios	Número de usuarios de red. Número de equipos en red. Cantidad de carpetas compartidas Información compartida en red que no necesita estarlo Porcentaje de información compartida a la que deben tener acceso los usuarios Pérdida de información	¿Existe un método para la autenticación de usuarios que acceden a la red de datos? ¿Existen políticas para la administración de usuarios (creación y eliminación)? ¿Existen políticas para compartir información? ¿Cuenta con políticas que especifique como proceder cuando un usuario necesita acceder a información compartida? ¿Tienen políticas de respaldo? ¿Cuentan con plan de contingencia y recuperación de desastres?	Encuesta Entrevista Observación
	Manejo de vulnerabilidad	Número de carpetas compartidas en red por equipo	¿Existe restricción de acceso a la información compartida (permisos lectura/escritura).	Encuesta Entrevista

	de la red informática	Número de equipos a los que se puede acceder sin contraseña	¿Cuántos computadores tienen contraseña?	Observación
		Número de equipos con contraseña en blanco	¿Cuántos equipos tienen contraseña en blanco?	
		Cantidad de contraseñas fáciles de deducir.	¿Cuántos equipos tienen contraseña relacionada con la información del usuario (identificación, nombre, apellido, nombre de hijo(a))?	
		Cantidad de equipos que cuentan con regulador/UPS	¿Cuántos equipos cuentan con regulador de voltaje/UPS?	
		Cantidad de equipos fáciles de sustraer	¿Cuántos servidores se encuentran protegidos por UPS?	
			¿Cuántos equipos tienen seguridades para evitar robo?	

3.1.3. **Objetivos**

3.1.3.1. Objetivo general.

PROPONER UNA AUDITORIA DE SEGURIDAD PARA EL MANEJO DE VULNERABILIDADES DE LA RED INFORMATICA DE LA UNIVERSIDAD SEÑOR DE SIPAN.

3.1.3.2. Objetivo específicos:

Caracterizar las vulnerabilidades de la red informática de la Universidad Señor de Sipan.

Diseñar auditoria de seguridad adaptado a la red informática de la Universidad Señor De Sipan.

3.2. **Tipo de estudio, diseño de investigación**

3.2.1. **Investigación Descriptiva – propositiva**

Acerca de qué es investigación descriptiva Namakforoosh (2000) dice que "... es una forma de estudio para saber quién, dónde, cuándo, cómo y porqué del sujeto de estudio". Siendo así, este nivel de investigación ayudó a determinar el porcentaje de usuarios afectados por el problema objeto de estudio de la presente investigación. Y es propositiva porque plantea una alternativa o propuesta de solución a la problemática encontrada.

3.3. **Población y muestra de estudio**

3.3.1. **Población:**

Según se definen que: "población es el total de los individuos o elementos a quienes se refiere la investigación, es decir, todos los elementos que vamos a estudiar, por ello también se le llama universo" (Hurtado & toro, 1998),

La población que se utilizara para este estudio estará conformada por la Red informática de la Universidad Señor de Sipan los cuales lo conforman:

ADMINISTRATIVA	1
ACTIVIDADES INTEGRADORAS	2
ADMISIÓN	10
ALMACEN	2
ALMACEN Y COMPRAS	1
ARCHIVO	2
AREX NEG INT	7
ASESORÍA LEGAL	2
AUDITORIA	3
AUDITORIO B	1
BIBLIOTECA	44
BIENESTAR Y SERVICIOS ESTUDIANTILES	1
BOLSA	1
BOLSA DE TRABAJO	2
BOLSA DE TRABAJO Y SEGUIMIENTO	1
CALL CENTER	11
CEDECON	1
CENTRO DE INVESTIGACIÓN DE MERCADO	4
CENTRO MEDICO	2
CENTRO UNIVERSITARIO CAJAMARCA	1
CENTRO UNIVERSITARIO LIMA	15
CENTRO UNIVERSITARIO TRUJILLO	1
CEPRE	3
CHOFERES	1
CONSULTORIO MEDICO	2
CONTABILIDAD	9
COOP INTERNACIONAL	2
COORDINACIÓN DE GRADOS Y TÍTULOS	1
COORDINACIÓN DE GRADOS Y TÍ• TULOS DE LA EAP INGENIERÍ• A DE SISTEMAS	1
DEAC	4
DEFENSORIA ADMINISTRATIVA	2
DEPORTES	2

DESARROLLO ACADEMICO	3
DIRECCION DE RESPONSABILIDAD SOCIAL UNIVERSITARIA	3
DTI COORDINACIÓN DE GRADOS Y TÍ• TULOS DE LA EAP INGENIERÍ• A DE SISTEMAS	4
EAP ADGE Y TRABAJO SOCIAL	1
EAP ADM PÚBLICA	5
EAP ADMINISTRACION	12
EAP ADMINISTRACIÓN PÚBLICA, NEGOCIOS INTERNACIONALES, CENTRO INVESTIGACIÓN FACEM	1
EAP ARQUITECTURA	2
EAP ARTES & DGE EAP COMUNICACIÓN	2
EAP CIENCIAS DE LA COMUNICACIÓN	4
EAP CONTABILIDAD	5
EAP CONTABILIDAD	2
EAP DERECHO	15
EAP DERECHO	2
EAP ENFERMERÍA	6
EAP ESTOMATOLOGIA	1
EAP INGENIERIA CIVIL	1
EAP INGENIERÍA ECONÓMICA	2
EAP PSICOLOGIA	8
EAP TURISMO	5
EAP INGENIERIAS0	1
ESTOMATOLOGÍA	6
FACULTAD DE DERECHO	2
FACULTAD DE HUMANIDADES	4
FACCSA	4
FACEM	3
FIAU	7
FIAU COORDINACIÓN DE GRADOS Y TÍ• TULOS EAP INGENIERÍ• A MECÁ• NICA ELÉCTRICA	1
FINANZAS DEL ALUMNO	9
FIREWALL	1

FORMACION GENERAL	13
FOTOCOPIADO	1
GERENCIA DE TALENTO HUMANO	10
GERENCIA COMERCIAL	1
GERENCIA GENERAL	2
GRADOS Y TITULOS	3
IMAGEN	6
INFORMES	1
INFRAESTRUCTURAS	3
INTEGRACION	2
JEFATURA DE RECURSOS	1
LABORATIO SISTEMAS	2
LABORATORIO DE SIMULADORES	1
LABORATORIO DE SIMULADORES	1
LABORATORIO DE SISTEMAS	1
LOGISTICA	1
LOGISTICA	1
LOGISTICA	1
MANTENIMIENTO	1
MARKETING	9
MEDICINA	5
MONITOREO	2
NEGOCIOS INTERNACIONALES	2
PARQUE CIENTIFICO TECNOLOGICO	1
PATRIMONIO	1
PLANIFICACION	2
POSGRADO	2
PRESIDENCIA	2
PROMOCION B LEARNING	1
PROMOCION EDUCACION A DISTANCIA	2
PROMOCION POSGRADO	3
PROMOCION PRE GRADO	10

RECEPCIÓN CLÍNICA	1
RECTORADO	4
RECUPERACIONES	1
RECURSOS INFORMÁTICOS	7
REGISTROS ACADÉMICOS	9
SALA DE DOCENTES ESCUELA DE DERECHO	1
SALA DOCENTES FACEM	9
SALA DOCENTES FIAU	1
Secretaria general	3
SECRETARIA ADMINISTRATIVA EAP INGENIERÍA INDUSTRIAL Y AGRO INDUSTRIAL	2
VICERECTORADO ACADÉMICO	8
Tutoría	4
Total de todo	404

TABLA 5: Población de todas las áreas de la Universidad señor de sipan

Fuente: elaboración propia

3.3.2. **Muestra:**

(Balestrini, 2006), señala que: “una muestra es una parte representativa de una población, cuyas características deben producirse en ella, lo más exactamente posible.”.

Dado que el número de elementos que comprenden la población es reducido no es necesario obtener una muestra por lo que en la presente investigación se trabajó con toda la población.

Para la elaboración de la muestra se ha usado la ecuación para determinar el tamaño de la muestra, para estimar una porción de población finita.

O=0.5

Z=1.96

E=0.04

N=404

$$N = \frac{\mathbf{N\,o^2Z^2}}{(\mathbf{N-1})\mathbf{e^2} + (\mathbf{o^2Z^2})}$$

$$N = \frac{}{(404-1)(0.04)^2 + (0{,}5)^2(1{,}96^2)}$$

N=242

De esta manera se obtiene que el tamaño de muestra para ser estudiada es de 242

3.4. **Métodos, técnicas e instrumentos de recolección de datos**

1. **Método**

Del análisis y pruebas técnicas con diferentes herramientas para medir el estado actual de la universidad señor de sipan, seguridad y automatización.

2. **Instrumentos.**

Herramientas como el software pilar, que nos ayudan a analizar nuestra red y Excel .

3. **La técnica de la observación:**

Permitirá verificar los hechos y dará un sello de transparencia e integridad a la investigación.

4. **La técnica de entrevista:**

Este método se utiliza para recabar información en forma verbal, a través de preguntas que propone el analista. Sirve para analizar la realidad y estado de la situación problemática.

5. **La técnica de la entrevista:**

Servirá para obtener la información requerida para cumplir con las funciones de los diferentes departamentos, junto con el personal que lo maneja. Para esto se realiza un cuestionario que será como instrumento para obtener la información requerida.

6. **La técnica del análisis documentario:**

Recolección de información a través de documentos existentes ya sean en libros, revistas, tesis e Internet entre otras.

7. **La técnica de consulta de usuarios**

Se consultará de forma formal o informal a expertos en Sistemas de Información.

8. **La técnica de la experimentación:**

Es un método que ayudara a estar más seguro de lo que se está realizando .Con esta técnica lo que se busca es una solución de calidad. Será de gran ayuda porque se obtendrá los datos relacionados a las diferentes características que posee cada uno

de los computadores es decir que se tendrá la información tanto de su software como de su hardware que tiene cada computador.

Procesamiento de datos y análisis estadísticos

Una vez realizadas las encuestas correspondientes, los resultados de la universidad señor de sipan, posteriormente serán documentados en una matriz de datos. Luego se tabularon los datos de la matriz por pregunta y posteriormente se realizaron tablas y gráficos correspondientes indicando los porcentajes y los resultados de cada pregunta para después poder llegar a las conclusiones correspondientes. A las personas que se les hizo la encuesta dieron sus respuestas de una forma que nos ayuda a ver el estado actual de los servicios brindados por parte de la red informática de la universidad señor de sipan y obtener las vulnerabilidades que están ocasionando el mal funcionamiento y generando problemas en los usuarios que utilizan este servicio para desempeñar sus labores en dicha universidad por lo tanto se realizó también una encuesta. Utilizaremos el EXCEL para gráficos y tablas.

IV. RESULTADOS

4.1. **Caracterizar las vulnerabilidades de la red informática de la universidad señor de sipán.**

4.1.1. **Cuestionario de Pregunta:**

1. ¿Cómo califica usted el servicio brindado por parte del área de la red informática?

TABLA 6: Encuesta Pregunta 01

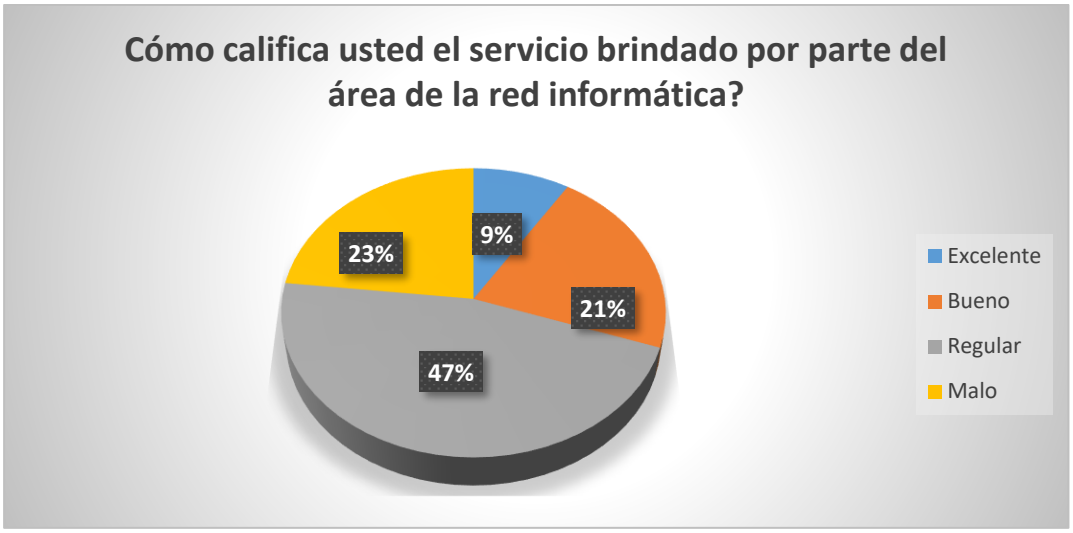
CATEGORIA	Frecuencia	porcentaje
Excelente	20	2%
Bueno	48	21%
Regular	114	54%
Malo	52	23%
Total	224	100%

Fuente: elaboración propia

De la tabla 6 podemos mencionar que de 224 personas, la mayor parte: Es decir 104 personas califican el servicio brindado como regular por parte del área de la red informática, 52 personas de ellas indican que el servicio es malo, 48 personas indican

que el servicio brindado es bueno y 20 personas indicaron que el servicio brindado es excelente por parte del área de la red informática.

Por lo tanto podemos notar que tiene problemas el área con el servicio brindado lo cual podemos ver te tiene vulnerabilidad al realizar este servicio.



Fuente: elaboración propia

2. ¿Está usted de acuerdo con la atención brindada por parte se servicio técnico?

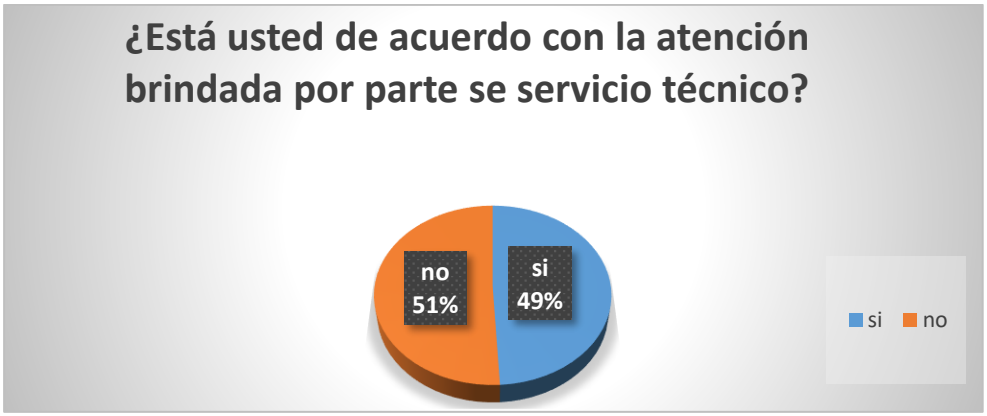
TABLA 7: Encuesta Pregunta 02

CATEGORIA	Frecuencia	porcentaje
si	110	49%
no	114	51%
toral	224	100%

Fuente: elaboración propia

En la tabla 7 en la siguiente pregunta las personas dieron sus respuestas sobre la atención del servicio técnico que brindan en la cual 114 personas indicaron que es malo y 110 personas indicaron que si es bueno el servicio técnico brindado.

En el siguiente grafico podemos notar los mismos resultado pero con porcentajes de las respuestas.



Fuente: elaboración propia

Este grafico nos da un alcance de ver la situación de como brinda el servicio técnico

3. ¿Con qué periodo se les da mantenimiento a las computadoras de su área?

TABLA 8: Encuesta Pregunta 03

CATEGORIA	frecuencia	Porcentaje
Mensual	64	29%
Semestral	100	45%
Anualmente	60	27%
Total	224	100%

Fuente: elaboración propia

En la tabla 8 en la siguiente pregunta las personas dieron sus respuestas sobre el periodo de mantenimiento de las computadoras en cada área y sus respuestas fueron. 100 personas respondieron que semestralmente realizan el mantenimiento de las computadoras, 64 personas respondieron que mensual dan mantenimiento y 60 personas respondieron anualmente le dan mantenimiento a las computadoras en su área

Fuente: elaboración propia

Este grafico nos da un alcance de ver la situación de como realizan el mantenimiento a las computadoras y en que periodos

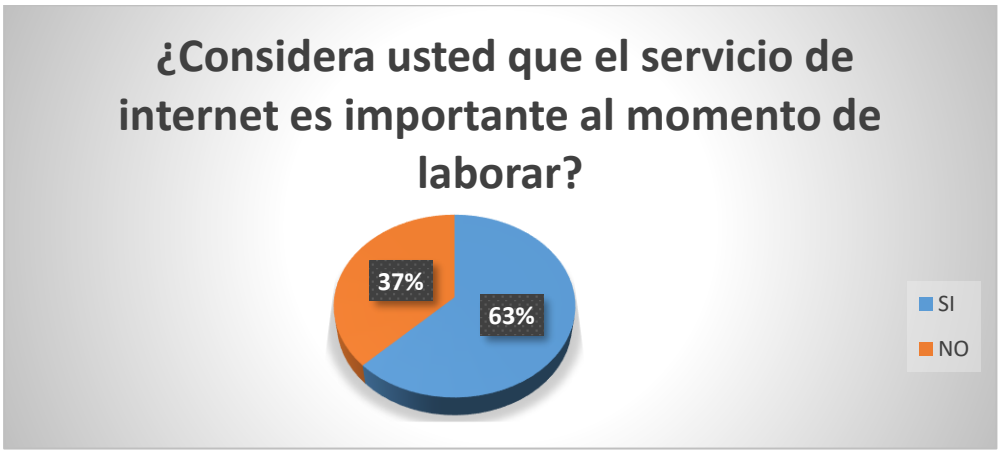
4. ¿Considera usted que el servicio de internet es importante al momento de laborar?

TABLA 9: Encuesta Pregunta 04

CATEGORIA	frecuencia	porcentaje
SI	134	63%
NO	80	37%
TOTAL	214	100%

Fuente: elaboración propia

En la tabla 9 en la siguiente pregunta las personas dieron sus respuestas sobre la importancia del internet en la cual, 134 personas respondieron que si es importante el internet y 80 personas respondieron que no era importante para ellos el internet porque no lo usabas.



Fuente: elaboración propia

Este grafico se puede observar los resultados de la importancia del internet en la cual nos da en porcentajes el 134 es equivalente al 63% de la parte azul del gráfico y el 80 es equivalente al 37% de la parte anaranjada como se muestra.

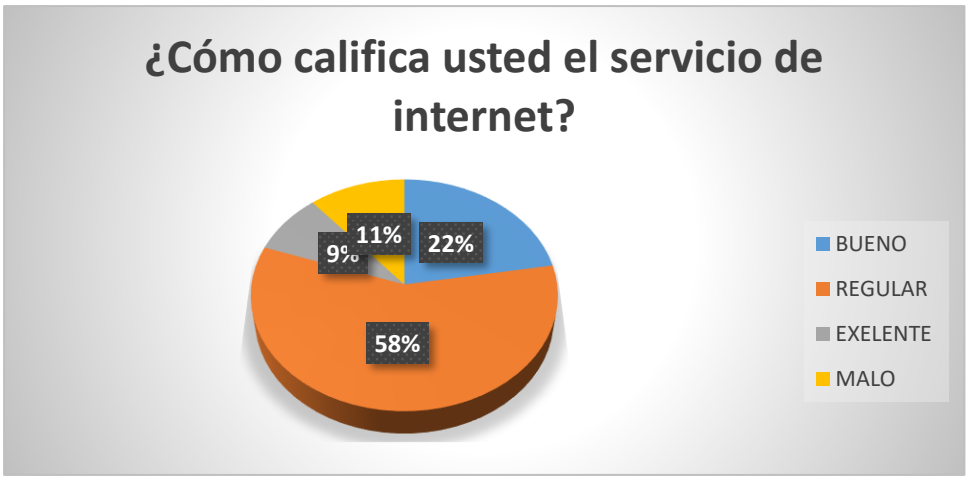
5. ¿Cómo califica usted el servicio de internet?

TABLA 10: Encuesta Pregunta 05

CATEGORIA	frecuencia	porcentaje
BUENO	50	22%
REGULAR	130	58%
EXELENTE	19	8%
MALO	25	11%
TOTAL	224	100%

Fuente: elaboración propia

En la tabla 10 en la siguiente pregunta las personas dieron sus respuestas de como califican el servicio de internet, 50 personas calificaron el servicio como bueno, 130 personas calificaron el servicio como regular, 19 personas calificaron el servicio como excelente y 25 personas calificaron el servicio como malo.



Fuente: elaboración propia

En Este grafico se puede observar los resultados de como califican el servicio del internet en la cual nos da en porcentajes el 50 es equivalente al 22% de la parte azul del gráfico, el 130 es equivalente al 58% de la parte anaranjada, 19 es equivalente al % de la parte ploma del gráfico y el 25 es equivalente al 11% de la parte amarilla del gráfico como se muestra.

6. ¿Tiene usted restricciones para ingresar a algún sitio web?

TABLA 11: Encuesta Pregunta 06

CATEGORIA	frecuencia	porcentaje
SI	190	85%
NO	34	15%
TOTAL	224	100%

Fuente: elaboración propia

En la tabla 11 en la siguiente pregunta las personas dieron sus respuestas si tendrían alguna restricción de las cuales 190 personas indicaron que si tienen restricciones y 34 personas indicaron que no tienen restricciones al ingresar a un sitio web por lo tanto se tendría en cuenta que sería vulnerable ante cualquier ataque o robo de información.

Fuente: elaboración propia

En Este grafico se puede observar los resultados de las restricciones que tienen para ingresar a un sitio web por lo tanto.190 es equivalente al 22% de la parte azul del gráfico que indican que si tienen restricciones y el 34 es equivalente al 15% de la parte anaranjada que indican que no tienen restricciones, como se indica en el gráfico mostrado.

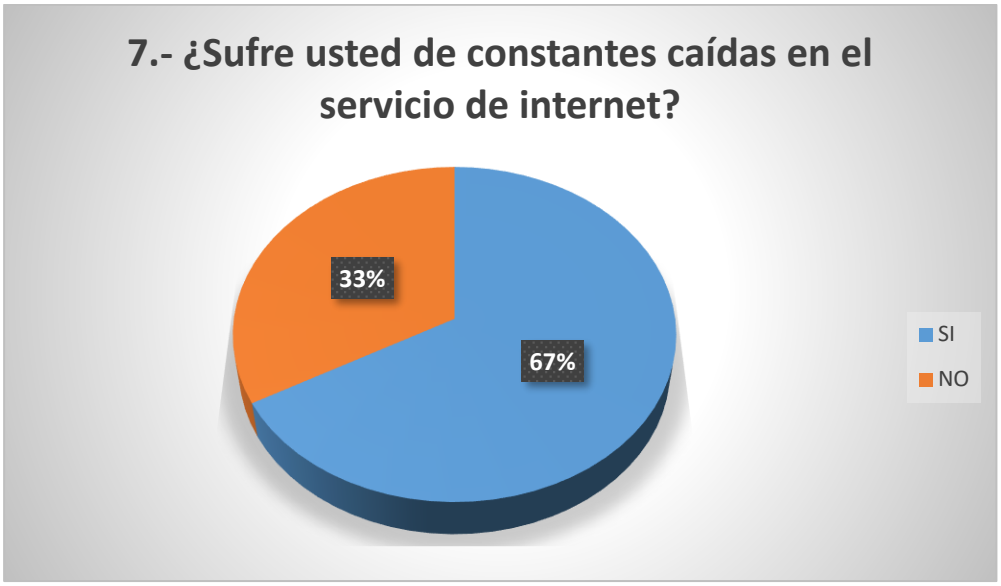
7. ¿Sufre usted de constantes caídas en el servicio de internet?

TABLA 12: Encuesta Pregunta 07

CATEGORIA	frecuencia	porcentaje
SI	150	67%
NO	74	33%
TOTAL	224	100%

Fuente: elaboración propia

En la tabla 12 en la siguiente pregunta las personas respondieron sobre las constantes caídas que tiene el servicio de internet en las cuales 150 personas tienen caídas del servicio y 74 personas no tienen caídas del servicio. Por lo que se puede ver que las caídas son frecuentes.



Fuente: elaboración propia

En Este grafico se puede observar los resultados de las constantes caídas que tiene el servicio de internet por lo tanto ,150 es equivalente al 67% de la parte azul del gráfico que indican que si tienen caídas y el 74 es equivalente al 33% de la parte anaranjada que indican que no tienen caídas constantes, como se indica en el gráfico mostrado.

8. ¿Cuál es el mayor problema que tiene al realizar su trabajo?

Cuando se va el internet y no puedo realizar mis labores o cuando se cuelgan Las computadoras y no se puede hacer nada tengo que estar llamando a la red para que solucione los problemas por lo tanto se pierde información y tiempo además las actualizaciones de los softwares no están actualizados.

4.1.2. **Entrevista.**

En la entrevista que se realizó a personas de la red informática señor de sipan nos dieron como respuesta de las siguientes preguntas q se le hizo si existe un método para la autenticación de usuarios y sus políticas de seguridad son deficientes para la administración de usuarios (creación y eliminación) además tiene un respaldo de políticas no muy confiable para realizar un plan de contingencia y recuperación de desastres lo cual pone en riesgo a la seguridad de las políticas. Pero si tiene restricciones de la información compartida como son:(permisos de lectura /escritura). Los equipos que tienen contraseñas relacionadas con la información del usuario (identificación, nombre, apellido, nombre) utilizan solo los que son autenticados con active directory. Es una tecnología de Microsoft para referirse a su implementación de servicio de directorio en una red distribuida que es usada por la red informática señor de sipan la cual cuenta con 26 servidores con regulador de voltaje/UPS y están debidamente protegidos gracias al ups pero no están protegidos contra algún robo o desastre natural que pueda ocurrir y dañar toda la parte física de la red informática estas fueron las respuestas del entrevistado por lo cual podemos notar que la red informática está muy vulnerable a diferentes problemas y desastres que pueden ocasionar el mal funcionamiento y perdida de información así como también perdidas económicas.

4.2. **En base al objetivo: desarrollo: diseñar auditoria de seguridad adaptado a la red informática de la universidad señor de sipán.**

4.2.1. **Se aplica la metodología Magerit mediante:**

Método de Análisis de riesgos (MAR)

Proceso de Gestión de riesgos (PGR)

Se procede a la adaptación de la estructura de procesos, actividades y tareas que plantea la metodología Magerit, ya antes mencionadas en el capítulo anterior, a la siguiente estructura diseñada para la presente tesis, ya que no todas las unidades de estudio son iguales.

Se Tiene en cuenta que se realiza un análisis cualitativo porque red informática de la Universidad señor de sipan no persigue ningún fin lucrativo, se puede decir que no recibe ningún pago por su USO, lo cual hace que el estudio no se centre en aumentar ganancias y disminuir perdidas sino que se plantea mejoras en la seguridad y manejo de vulnerabilidades y amenazas de la red informática de la Universidad señor de sipan.

El desarrollo del presente proyecto de análisis y gestión de riesgo de vulnerabilidades de la red informática de la Universidad señor de sipan, se realiza mediante la metodología Magerit y con el uso de la herramienta PILAR (7.1.9 - 31.5.2018) en su versión de prueba o de evaluación. Por lo cual se muestra el desarrollo de la metodología Magerit y a la par capturas de pantallas de su ejecución usando la herramienta Pilar.

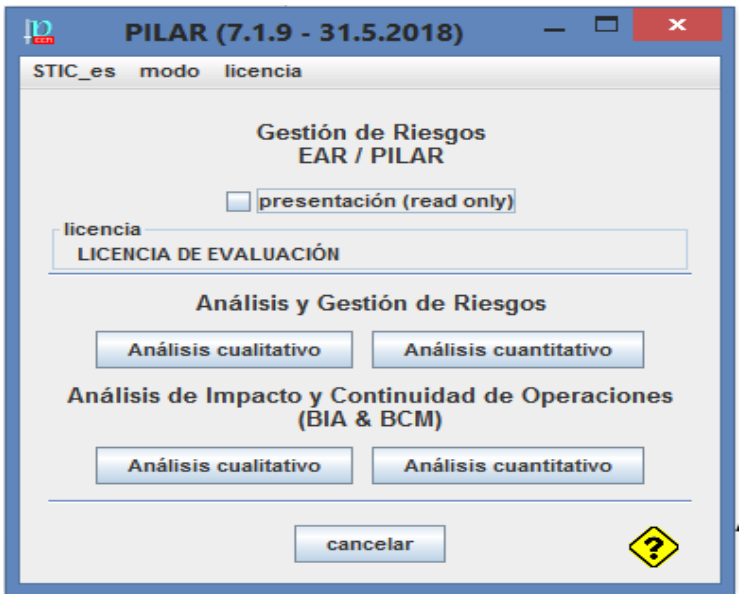


Figura 12: Datos Del Proyecto AUDITORIA-USS
Fuente: Obtenido de la ejecución del Proyecto con la herramienta Pilar (7.1.9 - 31.5.2018).
Elaborado: Br.adherly yeysson styven odar Guerrero.

4.2.2. **Datos Del Proyecto**

Código: AUDITORIA-USS

Nombre: SEGURIDAD Y MANEJO DE VULNERABILIDADES Y AMENAZAS DE LA RED INFORMATICA DE LA USS

Descripción: SEGURIDAD Y MANEJO DE VULNERABILIDADES Y AMENAZAS DE LA RED INFORMATICA DE LA UNIVERSIDAD SEÑOR DE SIPAN.

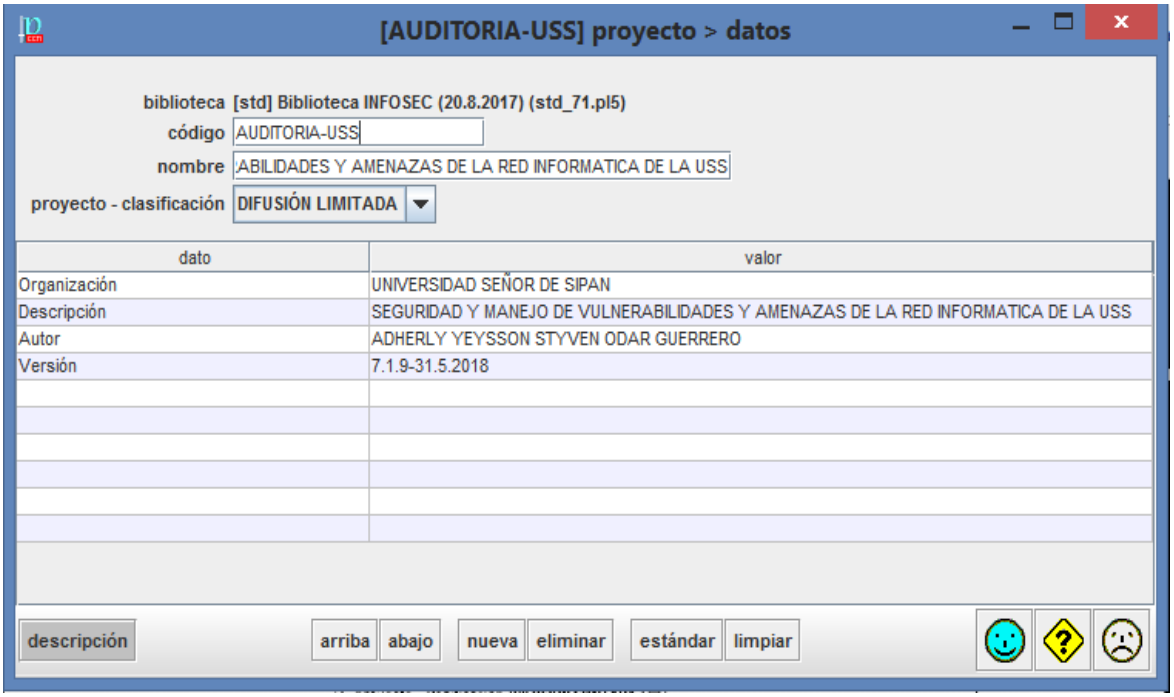


Figura 9: Datos Del Proyecto AUDITORIA-USS

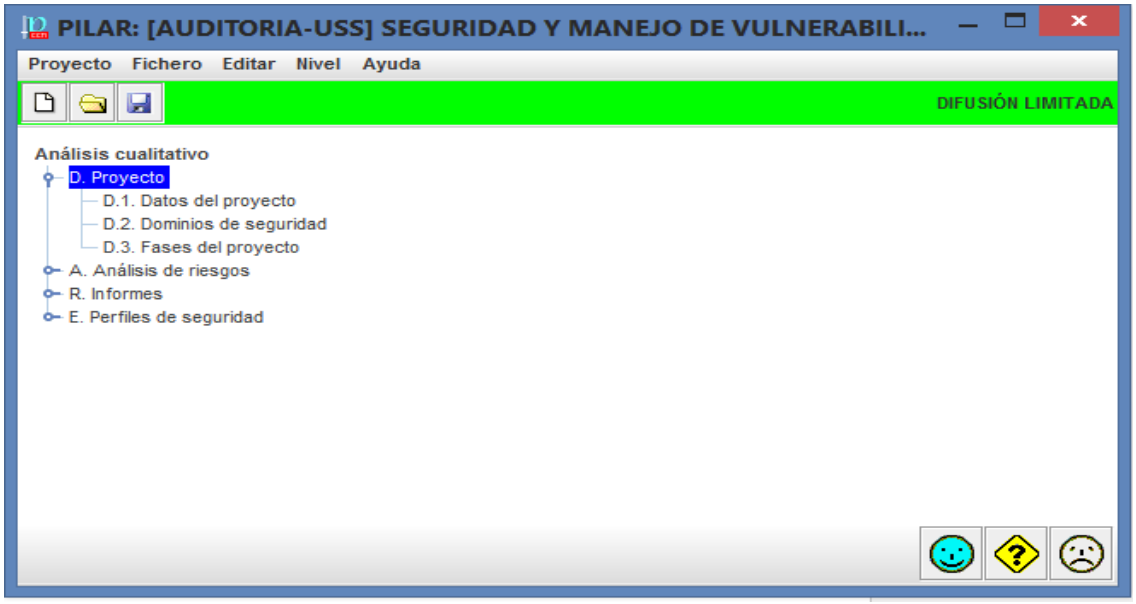
Fuente: Obtenido de la ejecución del Proyecto en la herramienta Pilar (7.1.9 - 31.5.2018).

Elaborado: Br.adherly yeysson styven odar Guerrero.

4.2.3. **Método de Análisis de Riesgos**

Para realizar la ejecución del proceso y la aplicación correcta de la metodología Magerit, el cual tiene como objetivos principales la identificación y estimación de los activos y de las posibles amenazas que asechan a la red informática, la recolección de la información fue obtenida a través de entrevistas, encuestas, aplicados a los

administradores del área de la red informática –USS .Este proceso se desarrollara a través de un análisis cualitativo por lo ya expuesto. A continuación una figura que muestra la pantalla de trabajo para el proceso de análisis de riesgos usando la



herramienta Pilar (7.1.9 - 31.5.2018).

Figura 13: Datos Del Proyecto AUDITORIA-USS

Fuente: Obtenido de la ejecución del Proyecto en la herramienta Pilar (7.1.9 - 31.5.2018).

Elaborado: Br.adherly yeysson styven odar Guerrero.

4.2.4. **MAR 1: Caracterización de los Activos**

El objetivo de las siguientes tareas específicas en esta actividad es reconocer los activos que componen los procesos y definir las dependencias entre ellos. Así mismo se realiza una valoración según la importancia que tenga cada activo para el caso de su estudio

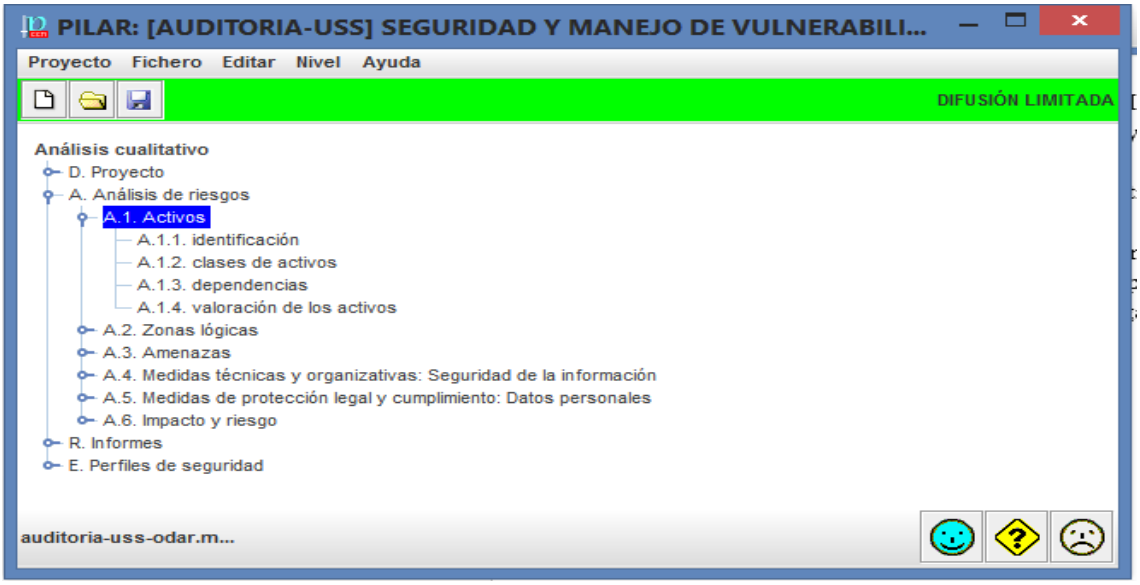


Figura 14: Datos Del Proyecto - AUDITORIA-USS -Activos

Fuente: Obtenido de la ejecución Del Proyecto en la herramienta Pilar (7.1.9 - 31.5.2018).

Elaborado: Br.adherly yeysson styven odar Guerrero.

4.2.5. **Tarea MAR 1.1: Identificación de los Activos**

La siguiente tarea tiene como objetivo, identificar los activos dentro del dominio, determinando sus características respectivas y atributos del activo a usar. Que son el código, nombre y una descripción breve de cada activo.

Para desarrollar la tarea se toma en cuenta los siguientes puntos:

Para el caso del código se considera 4 letras que en su mayor parte son las primeras letras de las palabras que forman su nombre de cada activo.

Los nombres se consideran con la actividad principal o el software que tenía instalados que formaban parte del objeto de estudio.

Para la descripción se considera el mismo caso que en el de los nombres.

El desarrollo que se realizara a través de la herramienta Pilar, basada en la metodología Magerit, facilita a la organización de los activos, mediante el uso de las capas generales, para el mejor entendimiento del objeto de estudio que se realizara, la estructuración mediante el tipo de activos, lo cual también permite usarla en la herramienta Pilar.

Los activos se agrupan en 8 capas según su tipo, como son servicios, software, hardware, redes de comunicaciones, soportes de información, equipamiento auxiliar, instalaciones y personal. A continuación se realiza la identificación de los activos para el Análisis de riesgos y vulnerabilidades que pueda tener en la actualidad la red informática de la universidad Señor de Sipan.

1. Lista de activos

1. [SW] Software

a. [SEUS] SISTEMA ESTANDARIZADO UNIVERSIDAD DE SIPAN

Se enfoca a la creación de una plataforma integral de Información.

Funciones:

Proporcionar soluciones tecnológicas para automatizar los procesos manuales.

Fortalecer el crecimiento modular del SEUSS para mejorar la gestión en la USS.

Administrar adecuadamente la Base de Datos, para estandarizar procedimientos de acceso dando mayor seguridad y confiabilidad a los datos.

Elaborar sistemas de información que permitan la integración del modelo dual que a la fecha tiene la USS, proyectándose a nuevos escenarios. Esta desarrollado bajo la plataforma visual estudio

2. **[HW] equipos**

Los medios materiales, físicos, destinados a soportar directamente o indirectamente los servicios.

3. **[SVIT] Servidores internos**

a. [SVDT] servidor de distribución.

Es la encargada de conectar redes locales independientes y controlar el tráfico que circula entre ellas. Está diseñada para interconectar redes, no hosts individuales.

b. [SVPX] servidor proxy: Es el servidor encargado de la validad de los acceso y permisos a la red de computadoras**.**

c. [SVAP] servidor de aplicaciones: Es el servidor encargado de almacenar las aplicaciones.

d. [SVAN] servidor antivirus: Es el servidor que brinda soporte at antivirus dentro de la red de computadoras.

e. [SVBK] servidor de backup: Es una copia de seguridad a mayor o menor escala.

f. [sebd] servidor de base de datos: Es el servidor que almacena la base de datos del sistema de gestión académica y todos los datos de la uss.

4. **[SVEX] Servidores externos:**

a. [SVCU] Servidor de Campus uss: Es el servidor donde se encuentra alojados todos los datos de los estudiantes y profesores para interactuar con el campus.

b. [SVCM] Campus Moodle: Es el servidor que se utiliza para guardas datos importantes de la Universidad e interactuar con el campus.

c. [SVWU] Servidor wed USS: Se utiliza para almacenar los archivos de un sitio y emitirlos por Internet para poder ser visitado por los usuarios.

d. [SVEP] Servidor EPUSS:

e. [SVCO] Servidor de correo: Este servidor se utiliza para la interacción de los usuarios, trabajadores de la Universidad ya que sin el no podrían comunicarse entre ellos, e intercambiar información.

5. **[SORE] Soporte de red:**

    a. [SWIT] Switch: Se utiliza para unir o conectar dispositivos en red.
    b. [FIRW] Firewall: Servidor que se configura y se administra el acceso y restricciones a las aplicaciones que se encuentran alojadas en los servidores de la USS y a internet.
    c. [ROUT] Router: Realiza el enrutamiento de la red y permite acceso at servicio de internet.

6. **[COM] Comunicaciones:** Incluye tanto instalaciones dedicadas como servicios de comunicaciones contratadas.

    a. [RLAN] red local: La red de la usss abarca todas las oficinas, que cuenten con equipos informáticos.
    b. [INTR] internet: Servicio brindado por terceros, a través de líneas dedicadas que son distribuidas para brindar diferentes servicios que se realizan en la Universidad.
    c. [SWAC] Switch de acceso: Permiten a su red adaptarse y admitir la implementación de nuevas aplicaciones para enfrentar las cambiantes necesidades empresariales.
    d. [SWDT] Switch de distribución: Se utiliza para combinar el tráfico VLAN y es un punto focal para las decisiones de política sobre flujo de tráfico en la red.
    e. [SWNU] Switch de núcleo: Funciona como agregado para el resto de los bloques de campus y une el campus con el resto de la red y nos proporciona el aislamiento de fallas y la conectividad de la troncal de alta velocidad de internet.

7. **[AUX] Equipamiento auxiliares:** Se consideran otros equipos que sirven de soporte
    a. [GRUE] Grupo electrógeno: Motor generador de energía que funciona cuando hay una pérdida de energía eléctrica o algún problema eléctrico.
    b. [EQAA] Equipo de aire acondicionado: Es un equipo de aire acondicionado encargado de mantener a una temperatura adecuada el data center.
    c. [UPSI] Sistemas de alimentación ininterrumpida: Sistema de alimentación ininterrumpida (UPS), encargados de brindar energía por un tiempo determinado a los servidores en caso que la energía eléctrica se pierda.
8. **[CABL] cableado:**
    a. [CAEL] cableado eléctrico: Conexiones del circuito eléctrico
    b. [CART] cableado de red: Conexiones de cables de comunicaciones
9. [L] **Instalaciones:**

    Son las conexiones que se realizaran para hacer uso de los quipos.

    a. [DC] Data center: Es el local de la USS de la Red, donde se encuentran los equipos que brindan los servicios y el personal encargado de tener en funcionamiento óptimo los equipos.

    2. [P] Personal
        a. [USUF] Usuarios Finales: Alumnos, docentes y Trabajadores Administrativos, Los alumnos que ingresan at portal web para matricularse, ver sus notas, etc.; el personal administrativo principalmente de las oficinas y dirección de escuelas.

b. [ADMC] administrador de comunicaciones y seguridad: Ing. Julio cesar Altamirano.

En la siguiente captura de pantalla se puede visualizar el ingreso de los activos que tiene la red informática de la Universidad señor de sipan a la herramienta pilar.

Al culminar la tarea se obtiene la lista de los 46 activos como se muestra en el siguiente imagen.

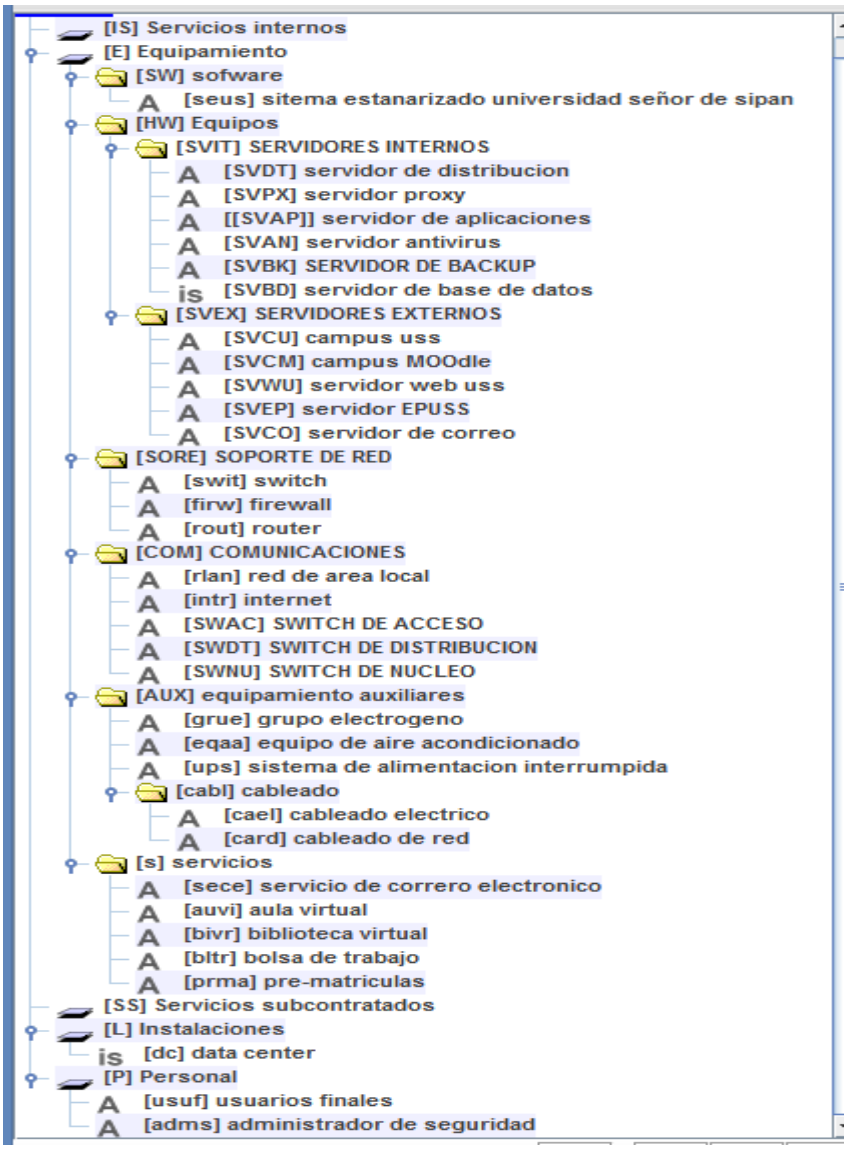


Figura 15: Lista de Activos - AUDITORIA-USS

Fuente: Se Obtiene De La Ejecución Del Proyecto En La Herramienta Pilar (7.1.9 - 31.5.2018).

Elaborado: Bachiller.adherly yeysson styven odar Guerrero.

4.2.6. **Tarea MAR 1.2: Dependencias entre los Activos**

Una vez los activos son identificados hay que valorar las dependencias entre activos, es decir la medida en que un activo de orden superior se puede ver perjudicado por una amenaza materializada sobre un activo de orden inferior.

En la siguiente tabla, teniendo en cuenta las dependencias para operar, funcionalidad y de almacenamiento de datos, se determina la siguiente matriz de dependencias entre activos (según el tipo de activos que corresponda):

	[SW]	[HW]	[SORE]	[COM]	[AUX]	[S]	[L]	[P]
[SW]	-							x
[HW]		-						x
[SORE]			-				x	X
[COM]				-			x	X
[AUX]					-		x	X
[S]	x	x	x	x	x	-	x	X
[L]							-	X
[P]								-

TABLA 13: Diagrama De Dependencia De Activos Según Su Tipo
Fuente: Elaboración propia basado en las actividades de la metodología Magerit.

Donde:

[SW]: Software

[HW]: Hardware

[COM]: Redes de Comunicaciones

[SORE]: Soporte de Red

[AUX]: Equipamiento auxiliar

[S]: Servicios

[L] Instalaciones

[P] Personal

El siguiente grafico muestra los activos y su dependencia, también Llamado mapa de dependencia entre activos en Pilar.

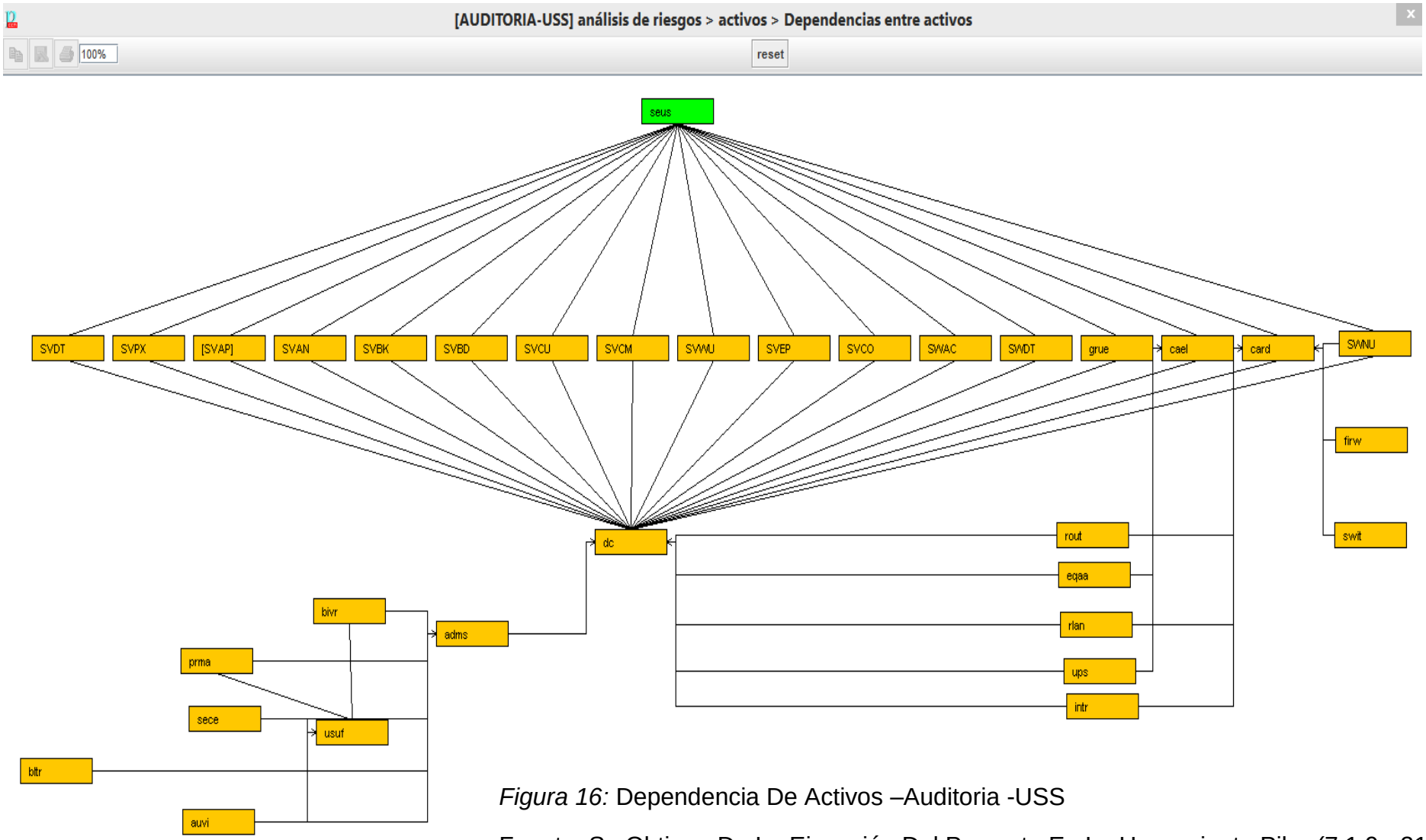


Figura 16: Dependencia De Activos –Auditoria -USS

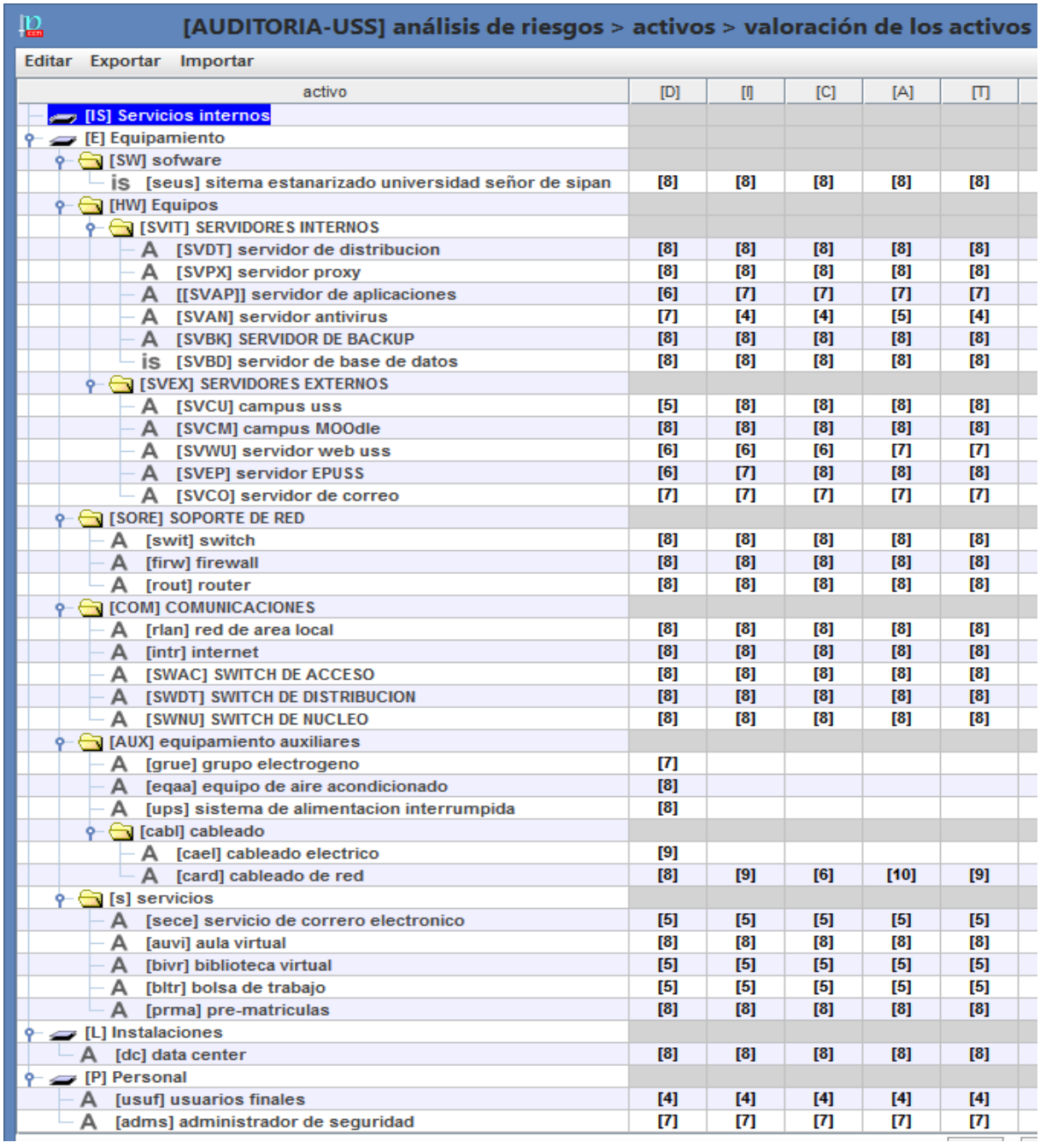
Fuente: Se Obtiene De La Ejecución Del Proyecto En La Herramienta Pilar (7.1.9 - 31.5.2018)

Elaborado: Br.adherly yeysson styven odar Guerrero.

4.2.7. **Tarea MAR 1.3: Valoración de los Activos**

La tarea tiene Como objetivos: Identificar en que dimensión es valioso el activo para la institución la estimación de la valoración en cada dimensión.

La valoración de los activos se muestra a continuación:



[AUDITORIA-USS] análisis de riesgos > activos > valoración de los activos

Editar Exportar Importar

activo	[D]	[I]	[C]	[A]	[T]
[IS] Servicios internos					
[E] Equipamiento					
[SW] sofware					
[seus] sitema estanarizado universidad señor de sipan	[8]	[8]	[8]	[8]	[8]
[HW] Equipos					
[SVIT] SERVIDORES INTERNOS					
[SVDT] servidor de distribucion	[8]	[8]	[8]	[8]	[8]
[SVPX] servidor proxy	[8]	[8]	[8]	[8]	[8]
[[SVAP]] servidor de aplicaciones	[6]	[7]	[7]	[7]	[7]
[SVAN] servidor antivirus	[7]	[4]	[4]	[5]	[4]
[SVBK] SERVIDOR DE BACKUP	[8]	[8]	[8]	[8]	[8]
[SVBD] servidor de base de datos	[8]	[8]	[8]	[8]	[8]
[SVEX] SERVIDORES EXTERNOS					
[SVCU] campus uss	[5]	[8]	[8]	[8]	[8]
[SVCM] campus MOOdle	[8]	[8]	[8]	[8]	[8]
[SVWU] servidor web uss	[6]	[6]	[6]	[7]	[7]
[SVEP] servidor EPUSS	[6]	[7]	[8]	[8]	[8]
[SVCO] servidor de correo	[7]	[7]	[7]	[7]	[7]
[SORE] SOPORTE DE RED					
[swit] switch	[8]	[8]	[8]	[8]	[8]
[firw] firewall	[8]	[8]	[8]	[8]	[8]
[rout] router	[8]	[8]	[8]	[8]	[8]
[COM] COMUNICACIONES					
[rlan] red de area local	[8]	[8]	[8]	[8]	[8]
[intr] internet	[8]	[8]	[8]	[8]	[8]
[SWAC] SWITCH DE ACCESO	[8]	[8]	[8]	[8]	[8]
[SWDT] SWITCH DE DISTRIBUCION	[8]	[8]	[8]	[8]	[8]
[SWNU] SWITCH DE NUCLEO	[8]	[8]	[8]	[8]	[8]
[AUX] equipamiento auxiliares					
[grue] grupo electrogeno	[7]				
[eqaa] equipo de aire acondicionado	[8]				
[ups] sistema de alimentacion interrumpida	[8]				
[cabl] cableado					
[cael] cableado electrico	[9]				
[card] cableado de red	[8]	[9]	[6]	[10]	[9]
[s] servicios					
[sece] servicio de correro electronico	[5]	[5]	[5]	[5]	[5]
[auvi] aula virtual	[8]	[8]	[8]	[8]	[8]
[bivr] biblioteca virtual	[5]	[5]	[5]	[5]	[5]
[bltr] bolsa de trabajo	[5]	[5]	[5]	[5]	[5]
[prma] pre-matriculas	[8]	[8]	[8]	[8]	[8]
[L] Instalaciones					
[dc] data center	[8]	[8]	[8]	[8]	[8]
[P] Personal					
[usuf] usuarios finales	[4]	[4]	[4]	[4]	[4]
[adms] administrador de seguridad	[7]	[7]	[7]	[7]	[7]

Figura 17: Valoración De Los Activos - AUDITORIA-USS

Fuente Se Obtiene De La Ejecución Del Proyecto En La Herramienta Pilar (7.1.9 - 31.5.2018)

Elaborado: Br.adherly yeysson styven odar Guerrero.

Se consideran dos datos importantes como dimensiones y criterios de valoración.

Dimensiones

[D] Disponibilidad

[I] Integridad de los datos

[C] Confidencialidad de los datos

[A] Autenticidad de los usuarios y de la información

[T] Trazabilidad del servicio y de los datos

Criterios de la valoración

Véase en la tabla 1 Escala detallada de los criterios de valoración.

El valor puede ser propio, o puede ser acumulado. Se dice que los activos inferiores en un esquema de dependencias, acumulan el valor de los activos que se apoyan en ellos.

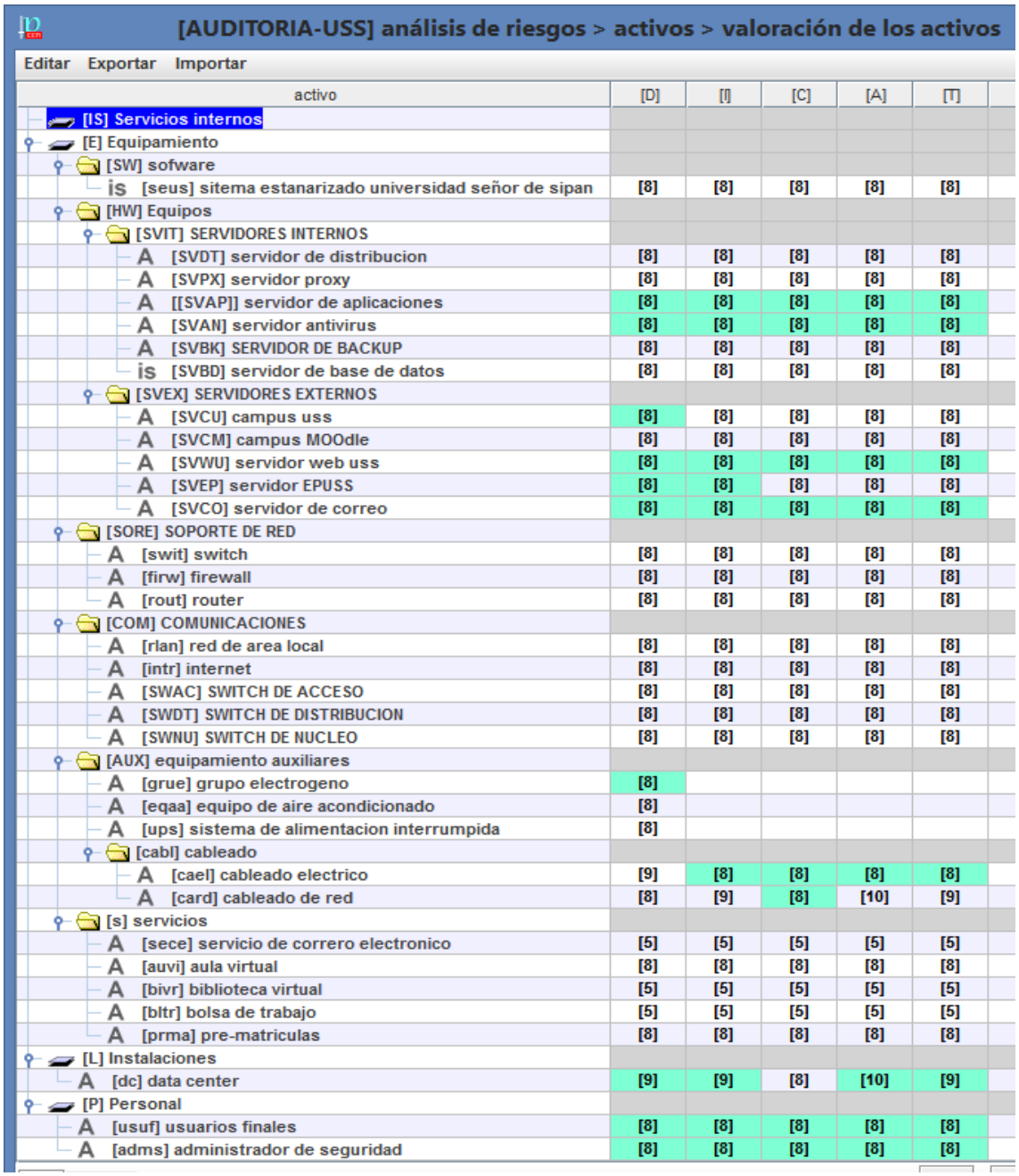
CRITERIOS	
Nivel 10	10
Nivel 9	9
Nivel Alto +	8
Nivel Alto	7
Nivel Alto -	6
Nivel Medio +	5
Nivel Medio	4
Nivel Medio -	3
Nivel Bajo +	2
Nivel Bajo	1
Sin Valor Apreciable	0

TABLA 14: Tabla De Criterios De Valoración-Pilar

Fuente: Obtenido De La Ejecución Del Proyecto En La Herramienta Pilar (7.1.9 - 31.5.2018).

Elaborado: Br.adherly yeysson styven odar Guerrero.

A continuación se puede ver el valor acumulado en la valoración de los activos



[AUDITORIA-USS] análisis de riesgos > activos > valoración de los activos

Editar Exportar Importar

activo	[D]	[I]	[C]	[A]	[T]
[IS] Servicios internos					
[E] Equipamiento					
[SW] sofware					
[seus] sitema estanarizado universidad señor de sipan	[8]	[8]	[8]	[8]	[8]
[HW] Equipos					
[SVIT] SERVIDORES INTERNOS					
[SVDT] servidor de distribucion	[8]	[8]	[8]	[8]	[8]
[SVPX] servidor proxy	[8]	[8]	[8]	[8]	[8]
[[SVAP]] servidor de aplicaciones	[8]	[8]	[8]	[8]	[8]
[SVAN] servidor antivirus	[8]	[8]	[8]	[8]	[8]
[SVBK] SERVIDOR DE BACKUP	[8]	[8]	[8]	[8]	[8]
[SVBD] servidor de base de datos	[8]	[8]	[8]	[8]	[8]
[SVEX] SERVIDORES EXTERNOS					
[SVCU] campus uss	[8]	[8]	[8]	[8]	[8]
[SVCM] campus MOOdle	[8]	[8]	[8]	[8]	[8]
[SVWU] servidor web uss	[8]	[8]	[8]	[8]	[8]
[SVEP] servidor EPUSS	[8]	[8]	[8]	[8]	[8]
[SVCO] servidor de correo	[8]	[8]	[8]	[8]	[8]
[SORE] SOPORTE DE RED					
[swit] switch	[8]	[8]	[8]	[8]	[8]
[firw] firewall	[8]	[8]	[8]	[8]	[8]
[rout] router	[8]	[8]	[8]	[8]	[8]
[COM] COMUNICACIONES					
[rlan] red de area local	[8]	[8]	[8]	[8]	[8]
[intr] internet	[8]	[8]	[8]	[8]	[8]
[SWAC] SWITCH DE ACCESO	[8]	[8]	[8]	[8]	[8]
[SWDT] SWITCH DE DISTRIBUCION	[8]	[8]	[8]	[8]	[8]
[SWNU] SWITCH DE NUCLEO	[8]	[8]	[8]	[8]	[8]
[AUX] equipamiento auxiliares					
[grue] grupo electrogeno	[8]				
[eqaa] equipo de aire acondicionado	[8]				
[ups] sistema de alimentacion interrumpida	[8]				
[cabl] cableado					
[cael] cableado electrico	[9]	[8]	[8]	[8]	[8]
[card] cableado de red	[8]	[9]	[8]	[10]	[9]
[s] servicios					
[sece] servicio de correro electronico	[5]	[5]	[5]	[5]	[5]
[auvi] aula virtual	[8]	[8]	[8]	[8]	[8]
[bivr] biblioteca virtual	[5]	[5]	[5]	[5]	[5]
[bltr] bolsa de trabajo	[5]	[5]	[5]	[5]	[5]
[prma] pre-matriculas	[8]	[8]	[8]	[8]	[8]
[L] Instalaciones					
[dc] data center	[9]	[9]	[8]	[10]	[9]
[P] Personal					
[usuf] usuarios finales	[8]	[8]	[8]	[8]	[8]
[adms] administrador de seguridad	[8]	[8]	[8]	[8]	[8]

Figura 18: Valoración De Los Activos-Valor Acumulado - AUDITORIA-USS

Fuente: Obtenido De La Ejecución Del Proyecto En La Herramienta Pilar (7.1.9 31.5.2018).

Elaborado: Br.adherly yeysson styven odar Guerrero.

4.2.8. **MAR 2: Caracterización de las Amenazas**

El objetivo es esta actividad de identificar las posibles amenazas que se pueden materializar sobre los activo y estimar la frecuencia de ocurrencia y degradación que la causa.

En la siguiente figura se muestra la pantalla de trabajo para realizar el siguiente paso que son las Amenazas. Se desarrollara usando la herramienta pilar tiene una opción para terminar la proporción de los factores que determinan las amenazas, para el estudio se utiliza la configuración predeterminada y se prosigue a la tarea siguiente.

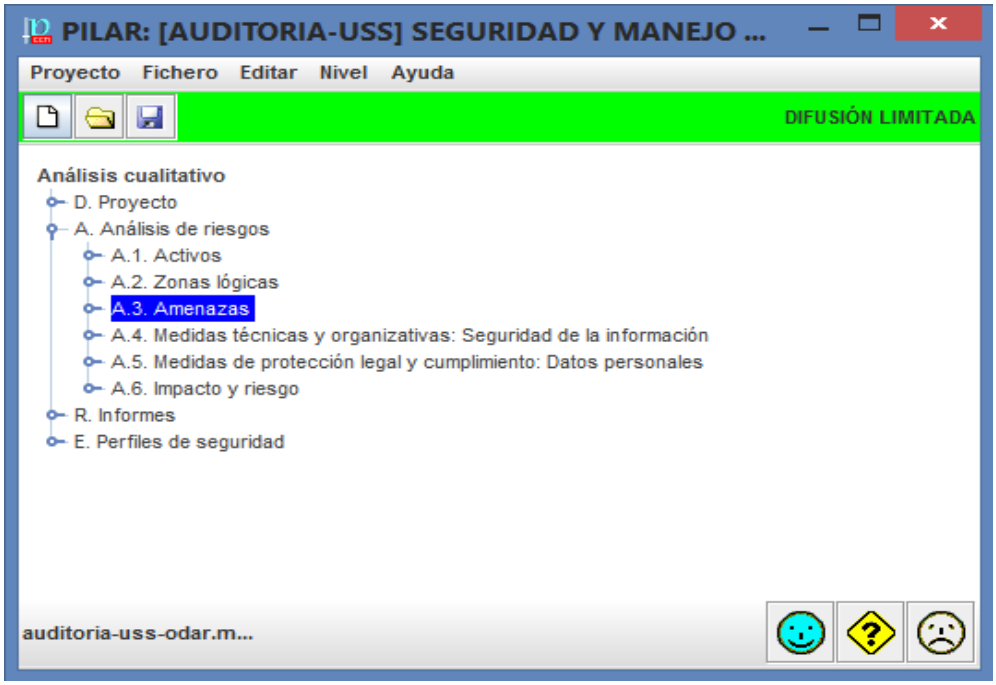


Figura 19: Pantalla De Trabajo En El Área De Amenazas.
Fuente: Obtenido De La Ejecución Del Proyecto En La Herramienta Pilar (7.1.9 31.5.2018).
Elaborado: Br.adherly yeysson styven odar Guerrero.

4.2.9. **Tarea MAR 2.1: Identificación de las Amenazas.**

El objetivo de la tarea es identificar las amenazas relevantes sobre cada activo. La herramienta pilar (7.1.9 31.5.2018). Estandarizada por Magerit. Las amenazas están clasificadas en.

Cuatro grupos:

[N] Desastres Naturales

[I] De Origen industrial

[E] Errores y fallos no intencionados

[A]Ataque deliberados

Se identifican las amenazas sobre cada activo, la siguiente lista muestra las amenazas que se identifican de la red informática de la universidad señor de sipan.

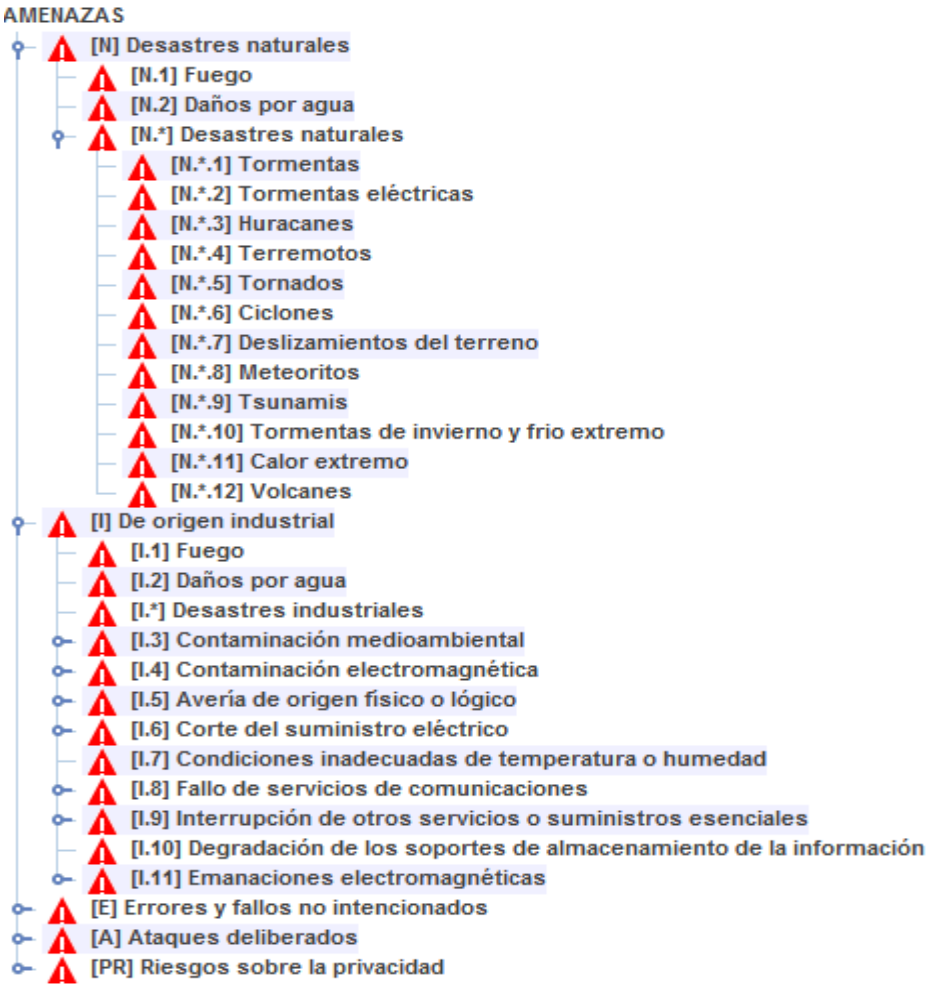


Figura 20: Área De Amenazas.

Fuente: Obtenido De La Ejecución Del Proyecto En La Herramienta Pilar (7.1.9 31.5.2018).

Elaborado: Br.adherly yeysson styven odar Guerrero.

El resultado de la Lista completa de las amenazas y los activos con sus respectivas amenazas se ubica en el Anexo. La lista de las Amenazas que se emplean en la Metodología Magerit y Herramienta Pilar (7.1.9 31.5.2018).

4.2.10. **Tarea MAR 2.1: Valoración de las Amenazas**

En la tarea Valoración de las Amenazas, se estima la frecuencia y la degradación de la materialización de las amenazas sobre cada activo identificado.

3. Probabilidad de ocurrencia: representa la tasa anual de ocurrencia, de cada activo cuanto se materializa una amenaza.
4. Porcentaje de degradación: significa el daño causado por un incidente.

La herramienta Pilar, tiene tablas de valores para la probabilidad de ocurrencia y el porcentaje de degradación, las cuales van a la par con las establecidas en la metodología Magerit. Realizan el estudio usando las tablas propuestas por la herramienta Pilar.

Como describir la probabilidad de que se materialice una amenaza

TABLA 15: Probabilidad

Potencia	Probabilidad	Nivel	Facilidad	Free.
XL extra grande	es casi seguro	MA muy alto	F fácil	100
L grande	MA muy alta	A alto	M medio	10
M medio	P posible	M medio	D difícil	1
S pequeño	PP poco probable	B bajo	MD muy difícil	0.1
XS muy pequeño	MR muy rara	MB muy bajo	ED extremadamente difícil	0.01

Fuente: obtenida del manual de usuarios de pilar (PILAR).

Como describir las consecuencias de la materialización de una amenaza.

TABLA 16: Degradación

Nivel		Porcentaje
T	total	100%
MA	muy alta	90%
A	Alta	50%
M	media	10%
B	Baja	1%

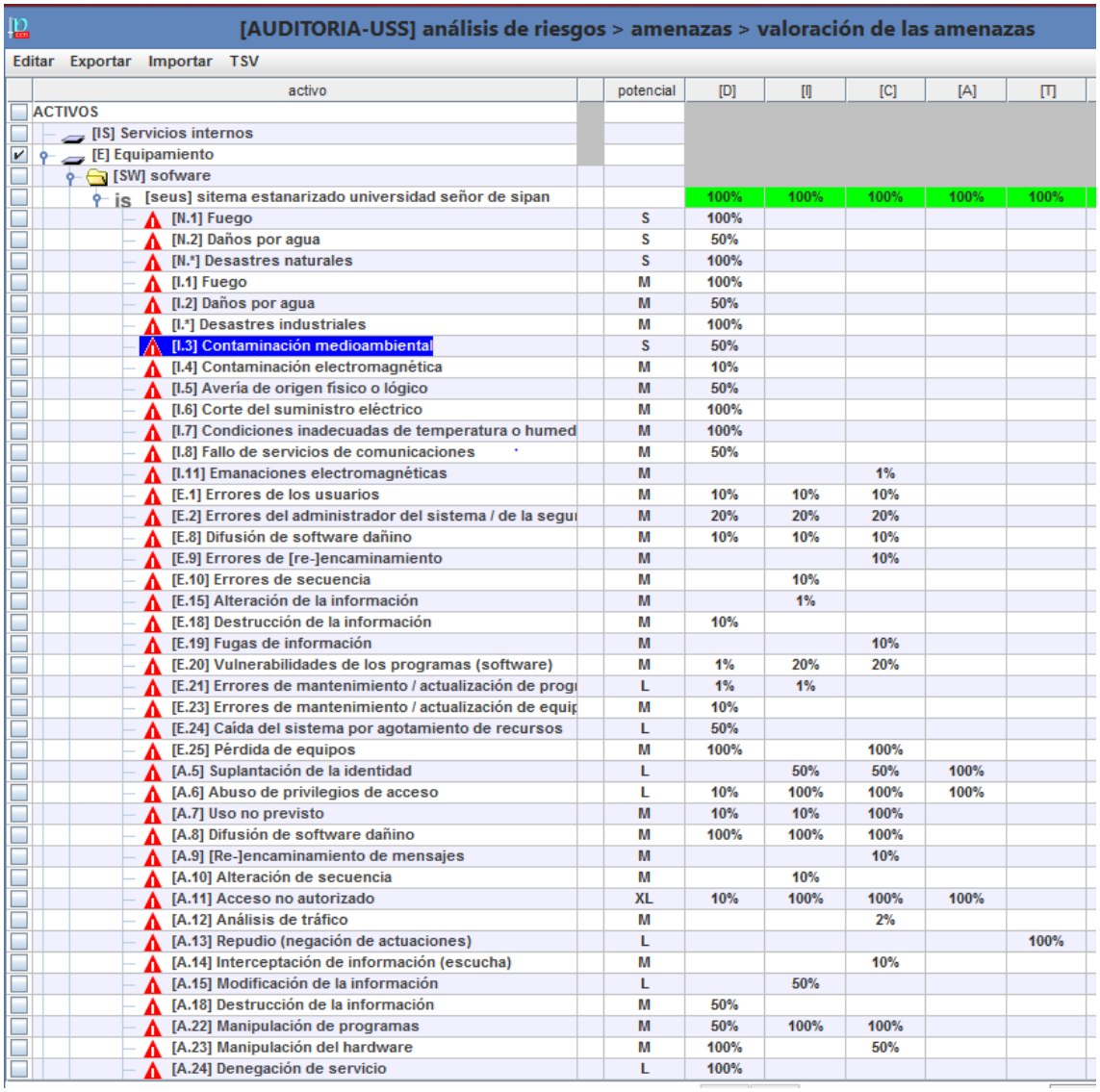
Fuente: obtenida del manual de usuarios de pilar (PILAR).

Luego esta degradación se extiende debido a la dependencia entre activos, Obteniendo el impacto y el riesgo, tanto acumulado como repercutido antes de aplicar las salvaguardas en la herramienta pilar. Si un activo A depende de otro B, el valor del impacto acumulado de A se acumula B en la proporción en la que depende. Por otro lado, el impacto repercutido indica que el daño en B en A en la proporción en la que A depende de B.

Impacto =Valor x Degradación

Riesgo= Impacto x Frecuencia

La Tabla muestra la valoración de las amenazas de los activos según sus dimensiones.



[AUDITORIA-USS] análisis de riesgos > amenazas > valoración de las amenazas

Editar Exportar Importar TSV

activo	potencial	[D]	[I]	[C]	[A]	[T]
ACTIVOS						
[IS] Servicios internos						
[E] Equipamiento						
[SW] sofware						
[seus] sitema estanarizado universidad señor de sipan		100%	100%	100%	100%	100%
[N.1] Fuego	S	100%				
[N.2] Daños por agua	S	50%				
[N.*] Desastres naturales	S	100%				
[I.1] Fuego	M	100%				
[I.2] Daños por agua	M	50%				
[I.*] Desastres industriales	M	100%				
[I.3] Contaminación medioambiental	S	50%				
[I.4] Contaminación electromagnética	M	10%				
[I.5] Avería de origen físico o lógico	M	50%				
[I.6] Corte del suministro eléctrico	M	100%				
[I.7] Condiciones inadecuadas de temperatura o humed	M	100%				
[I.8] Fallo de servicios de comunicaciones	M	50%				
[I.11] Emanaciones electromagnéticas	M			1%		
[E.1] Errores de los usuarios	M	10%	10%	10%		
[E.2] Errores del administrador del sistema / de la segu	M	20%	20%	20%		
[E.8] Difusión de software dañino	M	10%	10%	10%		
[E.9] Errores de [re-]encaminamiento	M			10%		
[E.10] Errores de secuencia	M		10%			
[E.15] Alteración de la información	M		1%			
[E.18] Destrucción de la información	M	10%				
[E.19] Fugas de información	M			10%		
[E.20] Vulnerabilidades de los programas (software)	M	1%	20%	20%		
[E.21] Errores de mantenimiento / actualización de prog	L	1%	1%			
[E.23] Errores de mantenimiento / actualización de equip	M	10%				
[E.24] Caída del sistema por agotamiento de recursos	L	50%				
[E.25] Pérdida de equipos	M	100%		100%		
[A.5] Suplantación de la identidad	L		50%	50%	100%	
[A.6] Abuso de privilegios de acceso	L	10%	100%	100%	100%	
[A.7] Uso no previsto	M	10%	10%	100%		
[A.8] Difusión de software dañino	M	100%	100%	100%		
[A.9] [Re-]encaminamiento de mensajes	M			10%		
[A.10] Alteración de secuencia	M		10%			
[A.11] Acceso no autorizado	XL	10%	100%	100%	100%	
[A.12] Análisis de tráfico	M			2%		
[A.13] Repudio (negación de actuaciones)	L					100%
[A.14] Interceptación de información (escucha)	M			10%		
[A.15] Modificación de la información	L		50%			
[A.18] Destrucción de la información	M	50%				
[A.22] Manipulación de programas	M	50%	100%	100%		
[A.23] Manipulación del hardware	M	100%		50%		
[A.24] Denegación de servicio	L	100%				

Figura 21: Valoración De Las Amenazas

Fuente: Obtenida De La Ejecución Del Proyecto En La Herramienta Pilar (7.1.9 31.5.2018).

Elaborado: Br.adherly yeysson styven odar Guerrero.

4.2.11. **MAR 3: Caracterización de las Salvaguardas**

En esta actividad se identificaran las salvaguardas efectivas para la red junto con la eficacia que tiene cada una de ellas para mitigar el riesgo. En el desarrollo de la metodología se definen varias etapas, para el estudio que se a determinado lo siguiente:

1. Primera etapa llamada POTENCIAL (potencial), desde el inicio de la creación del proyecto hasta la caracterización de amenazas.
2. Segunda etapa llamada SITUACIÓN ACTUAL (actual), toma los resultados de la primera etapa incluyendo la influencia de las salvaguardas implantadas hasta el momento.
3. Tercera etapa OBJETIVO (objetivo), recoge los datos de las dos etapas anteriores pero también hace referencia a los posibles resultados tras el plan de mitigación.

   Esta etapa se desarrolla en el proceso Gestión de Riesgos. En la herramienta pilar para el desarrollo de la actividad se toma en cuenta los Siguientes cuadros:

TABLA 17: Aspecto De Las Salvaguardas

Abreviaturas	Aspecto (que trata la salvaguarda)
G	para Gestión
T	para Técnico
F	para seguridad Física
P	Para gestión del Personal

Fuente: obtenida del manual de usuarios de pilar (PILAR).

TABLA 18: Tipo De Protección De Salvaguarda

Abreviatura	Tipo de protección de salvaguardas
PR	Prevención
DR	Disuasión
EL	Eliminación
IM	Minimización del impacto
CR	Corrección
RC	Recuperación
AD	Administrativa
AW	Concienciación
DC	Detención
MN	Monitorización

Fuente: obtenida del manual de usuarios de pilar. (PILAR)

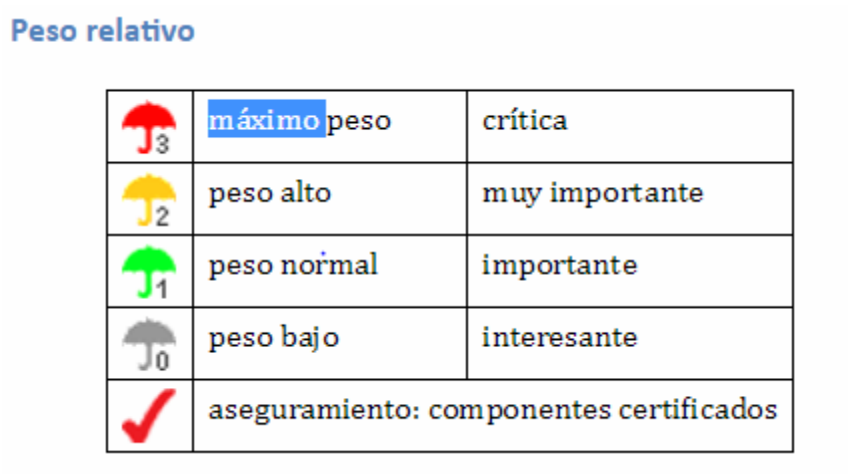


Figura 22: Peso Relativo

Fuente: Se obtienen Del Manual De Usuarios Pilar (PILAR).

4.2.12. Tarea MAR 3.1: Identificación de las Salvaguardas Existentes

En esta tarea se identifican las salvaguardas establecidas para proteger a los activos, utilizando la herramienta Pilar, se valora a través de las recomendaciones de la herramienta, que tan necesario es establecer una salvaguarda en un rango estimado de O a 10. Se considera el agrupamiento de Salvaguardas que realiza Magerit y Pilar, se explica cada agrupamiento de salvaguardas, por qué se escoge, sobre que activos se aplica, y a que amenazas enfrenta. Se identifica el grado de seguridad implementado en la institución, para ello se indaga una serie de aspectos generales e individuales considerando cada activo.

1. **Protecciones Generales.**

Se escoge esta salvaguarda por que define el uso controles y herramientas de identificación, autenticidad, monitorización de accesos. La salvaguarda se aplica sobre activos como : Servicios, Software, Hardware, Redes de Comunicaciones, Soportes de Información, Equipamiento auxiliar, Instalaciones y Personal . hace frente a amenazas como: Errores de los usuarios, Errores de administrador del sistema de la seguridad, difusión de software dañino, alteración de la información, errores de secuencia, alteración de la información, destrucción de la información, fugas de información, vulnerabilidades de los programas, perdida de equipos, indisponibilidad del personal, suplantación de la identidad, abuso de privilegios de acceso, uso no

previsto, acceso no autorizado, manipulación del software y manipulación del hardware.

2. **Protección de los Servicios.**

La salvaguarda plantea el aseguramiento de la disponibilidad, así como la gestión de cambios y aplicación de perfiles de seguridad buscando brindar un servicio con un alto grado de calidad. Hace frente a amenazas como: errores de los usuarios, errores del administrador del sistema de la seguridad, alteración de la información, fugas de información, caída del sistema por agotamiento de recursos, abuso de privilegios de acceso, uso no previsto, acceso no autorizado, destrucción de información y denegación de servicio.

3. **Protección de las aplicaciones informáticas.**

La salvaguarda plantea la gestión del uso y seguridad de los software utilizados para brindar el servicio final. Hace frente a amenazas como: errores de los usuarios, errores del administrador del sistema de la seguridad, difusión de software dañino, destrucción de la información, vulnerabilidad de los programas, errores de mantenimientos actualización, abuso de privilegios de acceso, uso no previsto y manipulación de programas.

4. **Protección de los equipos informáticos**

La salvaguarda plantea el aseguramiento de la disponibilidad, seguridad, mantener equipos operativos al aplicar cambios y operaciones. Hace frente a amenazas como: Desastres naturales, daños causados por fuego, agua, contaminación medioambiental, contaminación electromagnética, averías de origen físico o lógico, condiciones inadecuadas de temperatura o humedad, errores del administrador del sistema / de la seguridad, errores de mantenimiento actualización de equipos; caída del sistema por agotamiento de recursos, perdida de equipos, abuso de privilegios de acceso, uso no previsto, acceso no autorizado, manipulación de hardware y robo de equipos.

5. **Protección de las comunicaciones.**

La salvaguarda gestiona la integridad y confidencialidad de los datos intercambiados, el acceso al servicio, perfiles de seguridad, para ellos asegurar la disponibilidad y el correcto uso de las conexiones entrantes y salientes. Hace frente a vulnerabilidades como: fallo de servicios de comunicaciones, errores del administrador de sistema de la seguridad, errores de re encaminamiento, errores de secuencia, alteración de la información, fugas de información, caída del sistema por agotamiento de recursos, suplantación de la identidad, abuso de privilegios de acceso, uso no previsto, acceso no autorizado, análisis de tráfico, interceptación de información, modificación de la información, destrucción de la información y denegación de servicio.

6. **Protección de los soportes de información**

La salvaguarda gestiona la seguridad de los dispositivos físicos o documentos y la integridad de la información que almacenan. Hace frente a amenazas como: desastres naturales, desastres ocasionados por incendios, agua, industriales, contaminación medioambiental, avería de origen físico o lógico, degradación de los soportes de almacenamiento de la información, errores de los usuarios, alteración de la información, fugas de información, revelación de información y ataques destructivos.

7. **Elementos auxiliares**

La salvaguarda gestión la implementación de planes de seguridad que involucran al suministro eléctrico, la climatización y las protecciones del cableado de red. Hace frente a amenazas como: desastres naturales, desastres por fuego, agua, contaminación medioambiental, contaminación electromagnética, averías de origen físico o lógico, corte del suministro eléctrico, condiciones inadecuadas de temperaturas o humedad, errores de los usuarios, errores del administrador del Sistema de la seguridad, errores de mantenimiento, perdida de equipos, indisponibilidad del personal, uso no previsto, acceso no autorizado, robo de equipos y ataque destructivos.

8. **Protección de las Instalaciones**

La salvaguarda plantea el control de los accesos y el estado del diseño de los ambiente. Hace frente a amenazas como: desastres naturales, fuego, agua, contaminación ambiental, contaminación electromagnética, suplantación de identidad, abuso de privilegios de acceso, uso no previsto, acceso no autorizado, ataque destructivo y ocupación enemiga.

9. **Gestión del personal**

La salvaguarda plantea la formación y concienciación, disponibilidad del personal. Hace frente a amenazas como: alteración de la información, destrucción de la información, fugas de información, indisponibilidad del personal, extorción e ingeniería social.

10. **Adquisición/Desarrollo**

La salvaguarda plantea la compra o el desarrollo de aplicaciones, equipos informáticos, de comunicaciones, de soporte de información o comunicaciones que aporten a la mejora del servicio. Hace frente a amenazas como: errores de usuarios, errores del administrador del sistema de la seguridad, difusión de software dañino, alteración de información, fugas de información, vulnerabilidad de los sistemas, errores de mantenimiento actualización de programas, perdida de equipos, abuso de privilegios de acceso y uso no Previsto.

4.2.13. MAR 4: Estimación del Estado de Riesgo

En esta tarea se combinan los descubrimientos de las tareas anteriores para derivar Estimaciones del estado de riesgo de la Organización.

Esta actividad consta de tareas:

Estimación del impacto

Estimación del riesgo

El objetivo de estas tareas es disponer de una estimación fundada de lo que puede ocurrir (impacto) y de lo que probablemente ocurra (riesgo).

4.2.14. **Tarea MAR 4.1: Estimación del Impacto**

En esta tarea se estima el impacto al que están expuestos los activos:

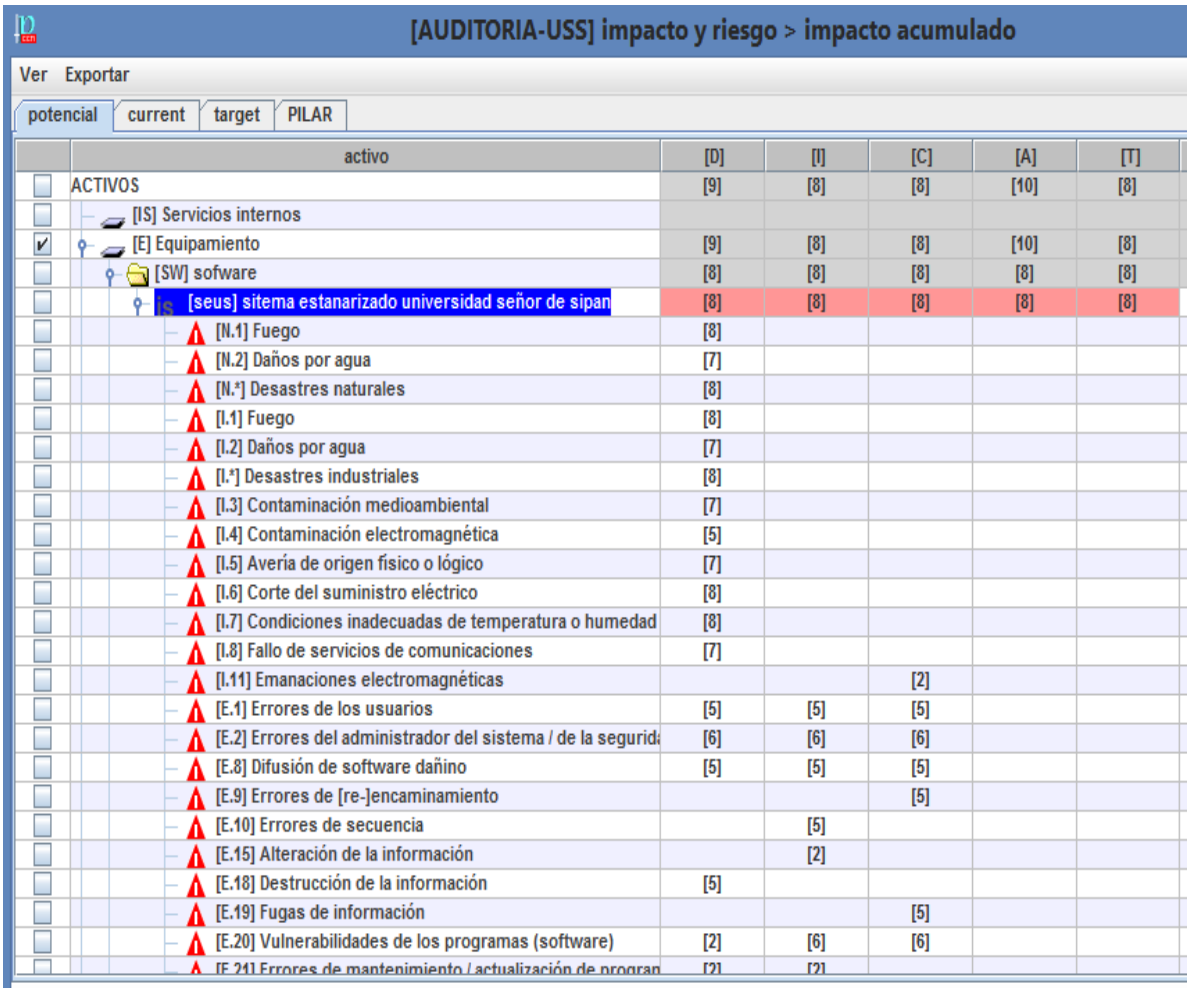
El impacto potencial, al que está expuesto el sistema teniendo en cuenta el valor de los activos y la valoración de las amenazas; pero no las salvaguardas actualmente desplegadas el impacto residual, al que está expuesto el sistema teniendo en cuenta el valor de los activos y la valoración de las amenazas, así como la eficacia de las salvaguardas actualmente desplegada.

TABLA 19: Estimación Del Impacto

CRITERIOS	
Nivel 10	10
Nivel 9	9
Nivel Alto +	8
Nivel Alto	7
Nivel Alto -	6
Nivel Medio +	5
Nivel Medio	4
Nivel Medio -	3
Nivel Bajo +	2
Nivel Bajo	1
Sin Valor Apreciable	0

Fuente: Manual del Usuario de Pilar.

Impactó Potencial Se denomina impacto a la medida del daño sobre el activo derivado de la materialización de una amenaza. Conociendo el valor de los activos (en varias dimensiones) y la de gradación que causan las amenazas, es directo al derivar el impacto que estas tendrían sobre el sistema. El impacto acumulado se calcula para cada activo, por cada amenaza y en cada dimensión de valoración, siendo una función del valor acumulado y de la degradación causada.



activo	[D]	[I]	[C]	[A]	[T]
ACTIVOS	[9]	[8]	[8]	[10]	[8]
[IS] Servicios internos					
[E] Equipamiento	[9]	[8]	[8]	[10]	[8]
[SW] sofware	[8]	[8]	[8]	[8]	[8]
[seus] sitema estanarizado universidad señor de sipan	[8]	[8]	[8]	[8]	[8]
[N.1] Fuego	[8]				
[N.2] Daños por agua	[7]				
[N.*] Desastres naturales	[8]				
[I.1] Fuego	[8]				
[I.2] Daños por agua	[7]				
[I.*] Desastres industriales	[8]				
[I.3] Contaminación medioambiental	[7]				
[I.4] Contaminación electromagnética	[5]				
[I.5] Avería de origen físico o lógico	[7]				
[I.6] Corte del suministro eléctrico	[8]				
[I.7] Condiciones inadecuadas de temperatura o humedad	[8]				
[I.8] Fallo de servicios de comunicaciones	[7]				
[I.11] Emanaciones electromagnéticas			[2]		
[E.1] Errores de los usuarios	[5]	[5]	[5]		
[E.2] Errores del administrador del sistema / de la seguridad	[6]	[6]	[6]		
[E.8] Difusión de software dañino	[5]	[5]	[5]		
[E.9] Errores de [re-]encaminamiento			[5]		
[E.10] Errores de secuencia		[5]			
[E.15] Alteración de la información		[2]			
[E.18] Destrucción de la información	[5]				
[E.19] Fugas de información			[5]		
[E.20] Vulnerabilidades de los programas (software)	[2]	[6]	[6]		
[E.21] Errores de mantenimiento / actualización de program	[2]	[2]			

Figura 23: Impacto Potencial

Fuente: Obtenida De La Ejecución Del Proyecto En La Herramienta Pilar (7.1.9 31.5.2018).

Elaborado: Br.adherly yeysson styven odar Guerrero.

4.2.15. **Tarea MAR 4.2 Estimación del Riesgo**

En esta tarea se estima el riesgo al que están sometidos los activos del sistema: el riesgo potencial, al que está sometido el sistema teniendo en cuenta el valor de los activos y la valoración de las amenazas; pero no las salvaguardas actualmente desplegadas. El riesgo residual, al que está sometido el sistema teniendo en cuenta

el valor de los activos y la valoración de las amenazas, así como la eficacia de las salvaguardas actualmente desplegadas.

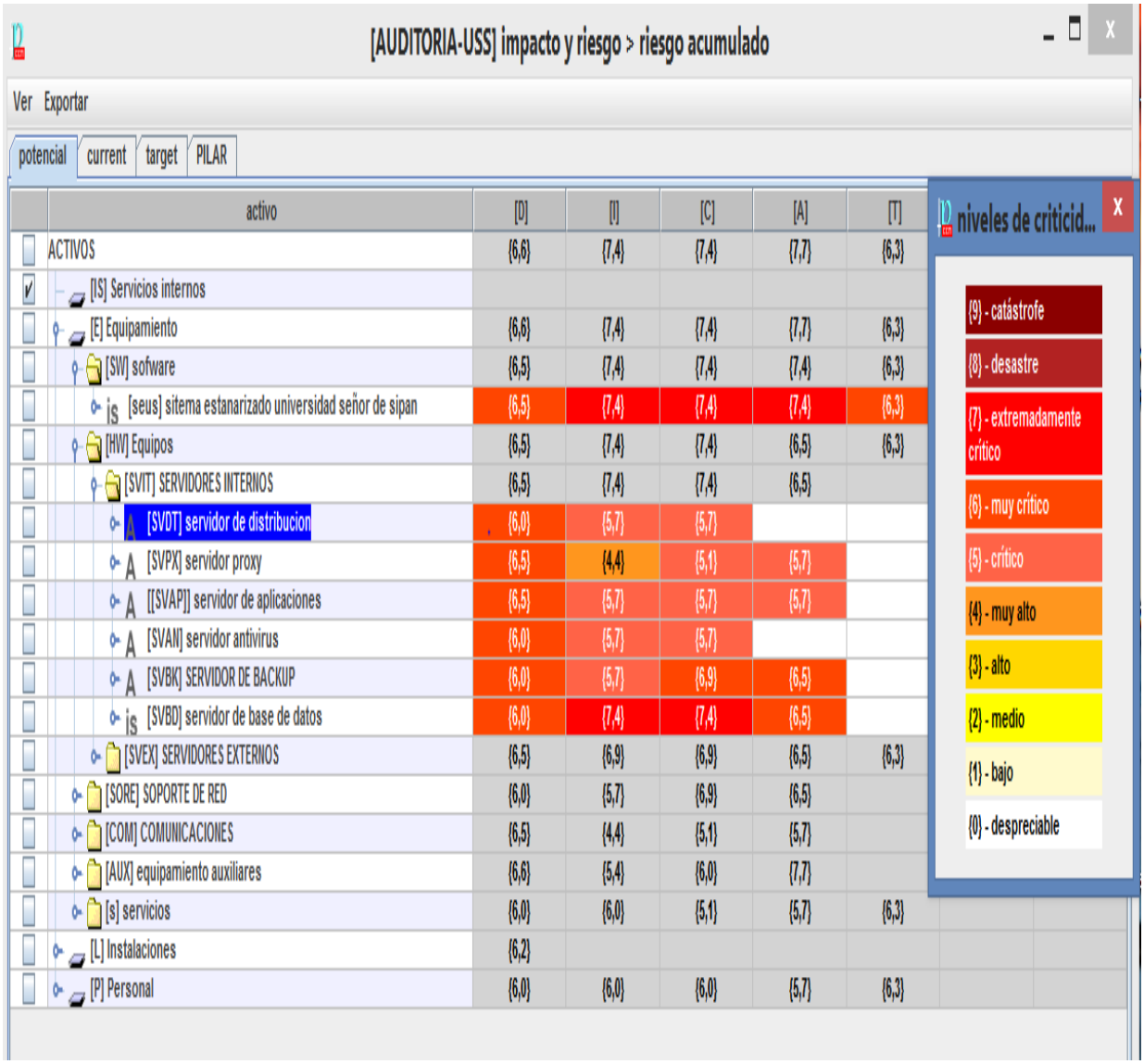


Figura 24: Estimación De Riesgo Acumulado

Fuente: Obtenida De La Ejecución Del Proyecto En La Herramienta Pilar (7.1.9 31.5.2018).

Elaborado: Br.adherly yeysson styven odar Guerrero.

Interpretación de los resultados

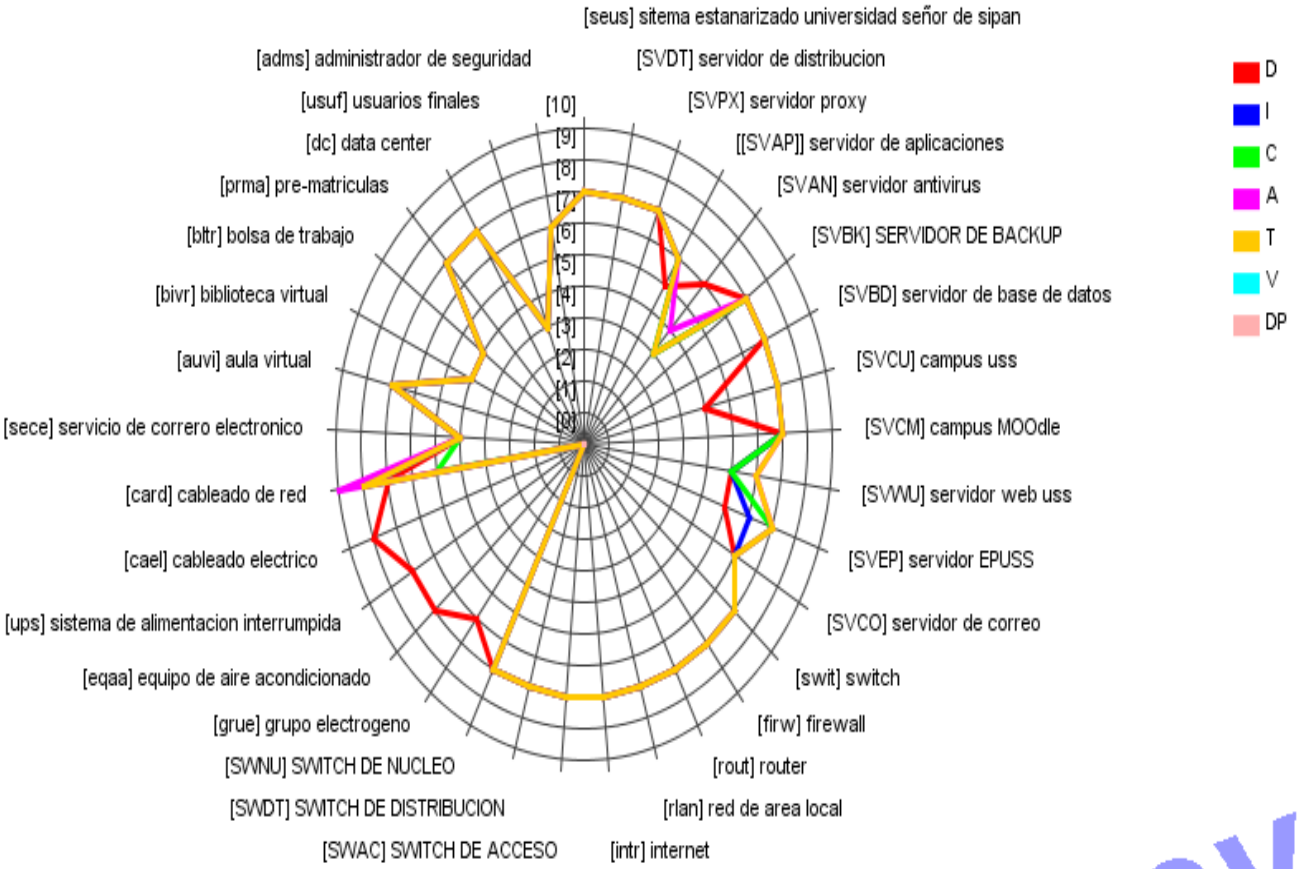


Figura 25: Identificación De Riesgos Por Activos

Fuente: Obtenida De La Ejecución Del Proyecto En La Herramienta Pilar (7.1.9 31.5.2018).

Elaborado: Br.adherly yeysson styven odar Guerrero.

En la figura se puede observar, los resultados de todas las actividades que se trabajaron sobre los activos, las amenazas y las salvaguardas. Como indica la herramienta pilar, la leyenda, se mide mediante colores que proporciona. la línea de color rojo son los riesgos que están expuestos los activos, en la siguiente etapa se representa por la línea de color azul, que es el resultado de la aplicación de las salvaguardas existentes, teniendo presente que se maximiza la presencia de amenazas para realizar un estudio de la situación actual de la universidad que se encuentra el objeto de estudio. Los activos con los niveles más altos son sin duda alguna el sistema estandarizado de la Universidad señor de sipan y los servidores

principales que participan en conjunto para generar los servicios y el funcionamiento de la red informática de la Universidad señor de sipan.

Proceso de Gestión de Riesgos

Realizado el método de análisis de riesgos se obtiene los siguientes resultados del impacto y riesgo que se están utilizando en los activos. Una calificación de cada riesgo significativo, determinándose si:

1. Es crítico en el sentido de que requiere atención urgente
2. Es grave en el sentido de que requiere atención
3. Es apreciable en el sentido de que pueda ser objeto de estudio para su tratamiento
4. Es asumible en el sentido de que no se van a tomar acciones para atajarlo

La opción 4, aceptación del riesgo, siempre es arriesgada y hay que tomarla con prudencia y justificación. Las razones que pueden llevar a esta aceptación son:

Cuando el impacto residual es asumible
Cuando el riesgo residual es asumible

el coste de las salvaguardas oportunas es desproporcionado en comparación al impacto y riesgo residuales La calificación de los riesgos tendrá consecuencias entre las tareas subsiguientes, siendo por lo tanto un factor básico para establecer prioridad relativa de las diferentes actuaciones.

Toma de Decisiones

Identificación de riesgos críticos

Seleccionamos los activos que poseen un nivel de riesgo mayor, por lo cual se podrá sustentar el tema de estudio que se plantea en la presente tesis, en la siguiente tabla se muestra

activo	[D]	[I]	[C]	[A]	[T]
ACTIVOS	{6,6}	{7,4}	{7,4}	{7,7}	{6,9}
[seus] sitema estanarizado universidad señor de sipan	{6,5}	{7,4}	{7,4}	{7,4}	{6,9}
[SVDT] servidor de distribucion	{6,0}	{5,7}	{5,7}		
[SVPX] servidor proxy	{6,5}	{4,4}	{5,1}	{5,7}	
[[SVAP]] servidor de aplicaciones	{5,4}	{5,1}	{5,1}	{5,1}	
[SVAN] servidor antivirus	{5,4}	{3,3}	{3,3}		
[SVBK] SERVIDOR DE BACKUP	{6,0}	{5,7}	{6,9}	{6,5}	
[SVBD] servidor de base de datos	{6,0}	{7,4}	{7,4}	{6,5}	
[SVCU] campus uss	{4,2}	{6,9}	{6,9}	{6,5}	
[SVCM] campus MOOdle	{6,0}	{6,9}	{6,9}	{6,5}	
[SVWU] servidor web uss	{4,8}	{4,5}	{5,7}	{5,9}	
[SVEP] servidor EPUSS	{4,8}	{5,1}	{6,9}	{6,5}	
[SVCO] servidor de correo	{5,9}	{5,4}	{5,1}	{5,1}	{5,7}
[swit] switch	{6,0}	{6,5}	{6,5}	{6,5}	
[firw] firewall	{6,0}	{6,5}	{6,9}	{6,5}	
[rout] router	{6,0}	{6,5}	{6,5}	{6,5}	
[rlan] red de area local	{6,0}	{6,5}	{6,5}	{6,5}	
[intr] internet	{6,0}	{6,5}	{6,5}	{6,5}	
[SWAC] SWITCH DE ACCESO	{6,5}	{4,4}	{5,1}	{5,7}	
[SWDT] SWITCH DE DISTRIBUCION	{6,5}	{4,4}	{5,1}	{5,7}	
[SWNU] SWITCH DE NUCLEO	{6,5}	{6,5}	{6,5}	{6,5}	
[grue] grupo electrogeno	{5,1}				
[eqaa] equipo de aire acondicionado	{6,0}				
[ups] sistema de alimentacion interrumpida	{6,0}				
[cael] cableado electrico	{6,6}				
[card] cableado de red	{6,0}	{5,4}	{4,8}	{7,7}	
[sece] servicio de correro electronico	{4,2}	{4,2}	{4,2}	{3,9}	{4,5}
[auvi] aula virtual	{6,0}	{6,0}	{6,0}	{5,7}	{6,3}
[bivr] biblioteca virtual	{4,2}	{4,2}	{4,2}	{3,9}	{4,5}
[bltr] bolsa de trabajo	{4,2}	{4,2}	{4,2}	{3,9}	{4,5}
[prma] pre-matriculas	{6,0}	{6,0}	{6,0}	{5,7}	{6,3}
[dc] data center	{5,7}				
[usuf] usuarios finales	{3,7}	{3,7}	{3,0}	{3,3}	{3,9}
[adms] administrador de seguridad	{5,1}	{5,0}	{5,4}		

Figura 26: Identificación Del Riesgo Crítico Actual

Fuente: Obtenida De La Ejecución Del Proyecto En La Herramienta Pilar (7.1.9 31.5.2018).

Elaborado: Br.adherly yeysson styven odar Guerrero.

Al gestionar los activos con riesgos críticos.

En la anterior tarea se identificaron los activos, como estaban organizados en grupos de activos de la red informática de la Universidad señor de sipan: [SW] software, [Hw] equipos,[SORE] soporte de red,[COM] comunicaciones,[AUX] equipamiento auxiliares,[S] servicios,[L] instalaciones ,[P] personal. Los grupos presentan valores de riesgo acumulado similares, también presentan amenazas similares con alto riesgo acumulado, por lo cual se generalizan indicando en los casos necesarios la diferencia en aplicar la salvaguarda, las salvaguardas ordenadas de mayor valor de riesgo a menor son:

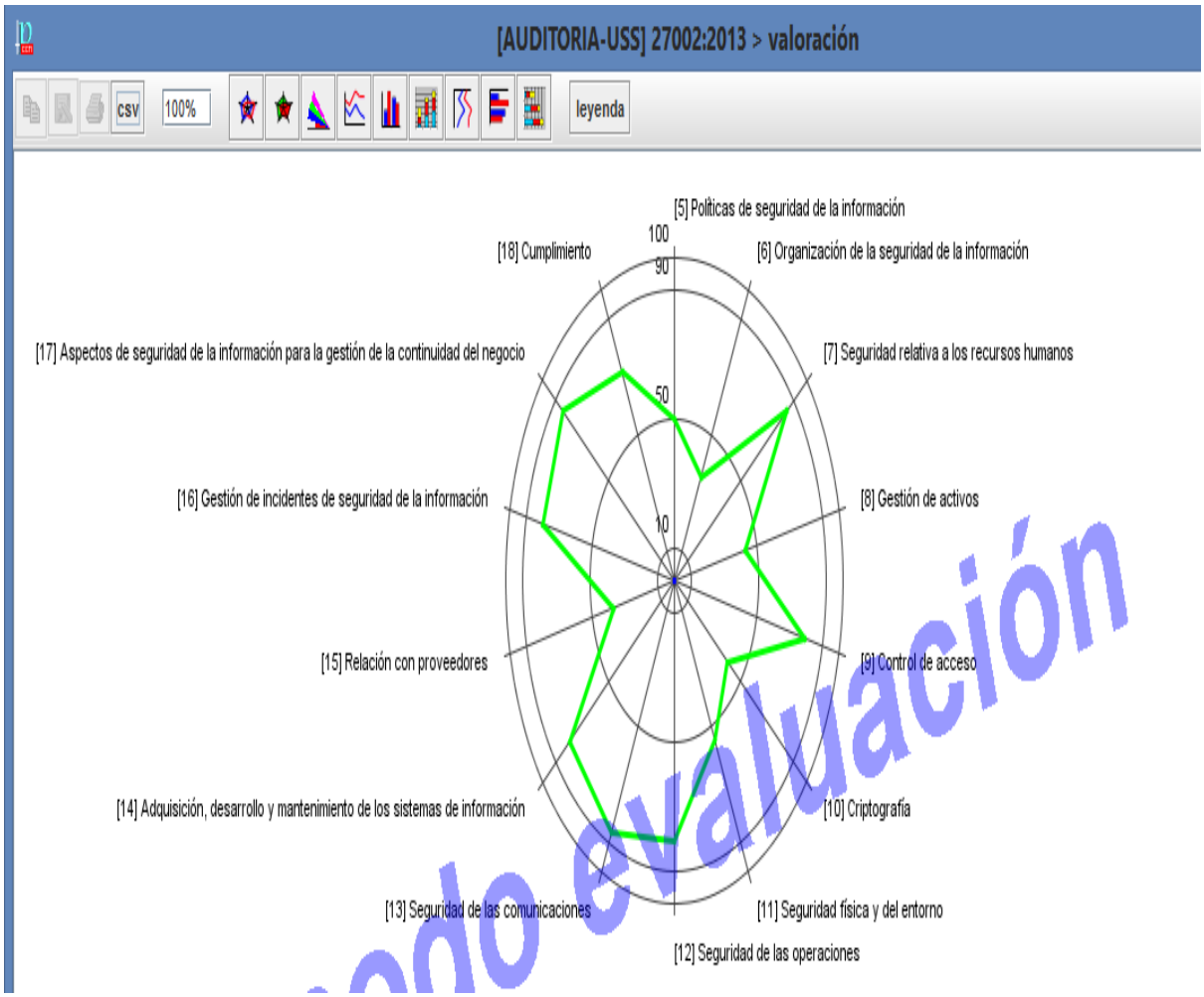


Figura 27: Gestión De Seguridad
Fuente: Obtenida De La Ejecución Del Proyecto En La Herramienta Pilar (7.1.9 31.5.2018)
Elaborado: Br.adherly yeysson styven odar Guerrero.

4.2.16. **Informe**

El Aporte para la siguiente investigación a la red informática de la universidad señor de sipán. Es Realizar La implementación del plan de mitigación para reducir las vulnerabilidades detectadas en el análisis de riesgos y se muestran en la siguiente figura. La línea de color verde lo representa.

Al realizar la elaboración del plan de mitigación, se consideran los siguientes aspectos, los activos que se trataran. Acciones y cronogramas.

A. Activos

Para el plan de mitigación, se lista a los activos que se utilizaran para mitigar en sus correspondientes planes de seguridad, para el desarrollo se incluyen casi todos los activos, principalmente con los que se involucran directamente con el objetivo de estudio que es la vulnerabilidad de la red informática de la universidad señor de sipán.

Lista de vulnerabilidades encontradas

Caída del sistema por agotamiento de recursos

Suplantación de la identidad del usuario

Denegación de servicio

Fuego

Daños por agua

Desastres naturales

Avería de origen físico o lógico

Corte del suministro eléctrico

Condiciones inadecuadas de temperatura o humedad

Abuso de privilegios de acceso

Acceso no autorizado

Existe documentación que no está actualizada.

Manipulación del hardware

Vulnerabilidad de los programas.

Errores de mantenimientos actualización.

Infecciones de Virus

Fallas en switches o Routers

Conectividad

Conclusiones:

Teniendo el resultado de la Auditoria se puede manifestar que se ha cumplido con evaluar las vulnerabilidades que tiene en la actualidad.

La red informática de la universidad señor de sipan presenta deficiencias sobre todo en el cumplimiento de Normas de Seguridad, porque no cumple las normas como es debido. Se debe destacar que el sistema no ha sido explotado en su totalidad.

Recomendaciones:

1. Elaborar un plan de emergencia que ayudé a contrarrestar de forma rápida y activa a caída del sistema por agotamiento de recursos.
2. Realizar un manual de seguridad que permita conocer a los usuarios que información deben proporcionar al momento de ingresar a sitios web.
3. Realizar mantenimiento periódico de los Sistemas y computadoras..
4. Elaborar un calendario de mantenimiento correctivo y preventivo de rutina periódico.
5. Elaborar toda la documentación técnica correspondiente a los Sistemas implementados y establecer normas procedimientos para las implementaciones y actualización.
6. Crear nuevas políticas de seguridad para el correcto uso de sistemas informáticos y se debe actualizar la documentación y el manual de políticas de seguridad,
7. Tener en mente que la información es el activo más importante de la red informática y por eso se debe considerar como un coste necesario.

B. Cronograma

Se estimara un tiempo aproximado 6 meses de la duración de la implementación o terminación de las actividades, planes o controles .que se utilizaran para mitigar las vulnerabilidades detectadas en la red informática de la universidad señor de sipán.

C. Aspectos

Como objetivo se busca mitigar riesgos, para mejorar la seguridad y vulnerabilidades de la red informática de la universidad señor de sipán.

El plan de mitigación tiene 4 aspectos generales:

1. Evitar: para eliminar las condiciones que permiten que el riesgo esté presente en todos los activos.
2. Aceptación: reconocer la existencia de las vulnerabilidades, pero no tomar ninguna acción para resolverla, a excepción del desarrollo posible de los planes de contingencia.
3. Mitigación: para reducir al mínimo la probabilidad de una ocurrencia del riesgo o el impacto ya existente.
4. Desviación: para transferir el riesgo parcial o total, si el caso lo diera.

Con los elementos mencionados se procede a elaborar el Plan de Mitigación.

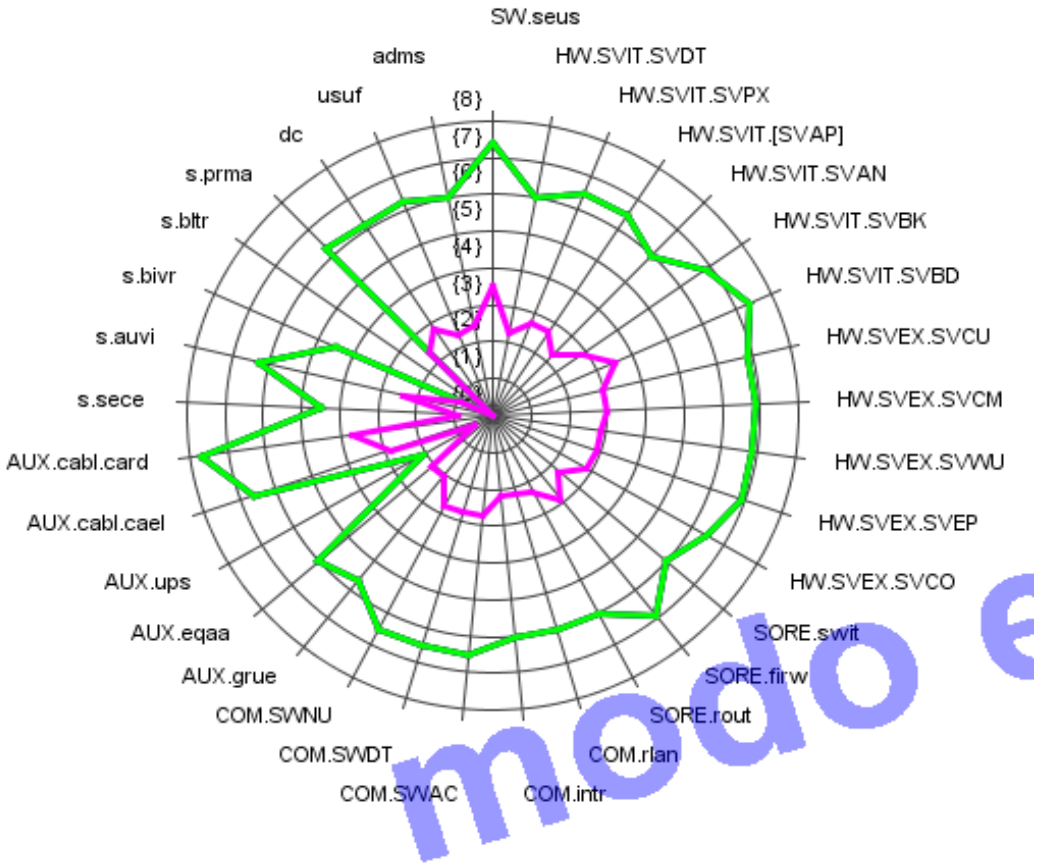


Figura 28: Reducción De Riesgos, Amenazas, Vulnerabilidades y Soluciones
Fuente: Obtenida De La Ejecución Del Proyecto En La Herramienta Pilar (7.1.9 31.5.2018).
Elaborado: Br.adherly yeysson styven odar Guerrero.

LA red informática de la universidad señor de sipan tiene que tener presente la investigación realizada en el siguiente trabajo la cual tuvo como diagnostico obtener las vulnerabilidades que afectan el funcionamiento y desempeño. Logrando obtener un informe para mitigar problemas futuros que pueden suceder y solucionarlos conjuntamente con la dirección de la red informática de la universidad señor de sipan.

V. DISCUSION.

Los resultados tienen relación con lo que sostiene (larrea Bustos & Yangua Jumbo, 2014) En su investigación denominada “Auditoría Informática y su Incidencia en los Riesgos para el manejo de la Información en la Cooperativa de Ahorro y Crédito Educadores de Tungurahua”, cuyo objetivo es (Determinar de qué manera la ineficiente Auditoría Informática influye en los riesgos para el manejo de la información en la Cooperativa de Ahorro y Crédito Educadores de Tungurahua.) de los resultados obtenidos(es tener conocimiento de cómo se encuentra la empresa actualmente, las conclusiones indican que(La mayoría de los empleados tienden a utilizar la misma contraseña de seguridad y la comparten con personas de su confianza, lo cual causaría graves problemas en la Seguridad de la Información y conduciría una falta de control de Seguridad dentro de la Empresa .

A partir de los resultados encontrados guardan relación con lo que sostiene (Ruiz Banda & Acosta Jordán, 2016)En su investigación denominada “Auditoría informática para la optimización del funcionamiento del de los sistemas informáticos de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial”, cuyo objetivo es (Realizar una Auditoría Informática para optimizar el funcionamiento de los sistemas y equipos informáticos de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial) los resultados obtenidos (La aplicación de pruebas sustantivas y de cumplimiento pudo demostrar que los equipos informáticos tienen un buen funcionamiento y son de gran utilidad para los estudiantes de la Facultad, las herramientas de hardware y software son estudiados e instalados al inicio de cada semestre según las necesidades cada laboratorio de las diferentes carreras).las conclusiones indican que(La aplicación de pruebas sustantivas y de cumplimiento pudo demostrar que los equipos informáticos tienen un buen funcionamiento y son de gran utilidad para los estudiantes de la Facultad, las herramientas de hardware y software son estudiados e instalados al inicio de cada semestre según las necesidades cada laboratorio de las diferentes carreras.

VI. CONCLUSIONES.

En el presente trabajo Se realizó un análisis de riesgos e impactos para ver las vulnerabilidades de la red informática además se describe los conceptos e importancia relacionada en la auditoria informática de seguridad de los diversos equipos, servicios y personal del área de TI con el uso de la herramienta pilar utilizando la metodología Magerit enfocándose en los activos de toda la red para ver y caracterizar su estado actual. Se identificaron los factores influyentes mediante el uso de la herramienta pilar (7.1.9 31.5.2018) y fue implementada la metodología Magerit en el caso de estudio realizado para conocer las vulnerabilidades a los cuales se encuentran expuestos los activos que forman parte de la red informática en la cual se realizó la auditoria de orden cualitativo que permitió ver el nivel de seguridad aplicada a la red. Posteriormente se utilizan las salvaguardas necesarias para reducir los niveles de vulnerabilidad, realice una correcta supervisión de estos procesos para brindar un mayor aseguramiento de las políticas.

Se logró determinar las vulnerabilidades con la metodología Magerit que se utilizó y la herramienta pilar que usa la iso 27002-2013,al proponer un diseño de una auditoria de seguridad se pudo realizar las evaluaciones referentes a los activos, amenazas ,vulnerabilidades que está expuesta y salvaguardas para finalmente obtener los niveles de riesgo e impacto plasmados en gráficas radiales permitiendo la identificación para implementar procedimientos y normas cuya finalidad sea la protección de los recursos e información. La herramienta pilar determino las vulnerabilidades que tiene la red informática para poder mitigar y disminuir los daños con salvaguardas que solucionan las vulnerabilidades detectadas en este estudio lo cual sustentada la problemática expuesta y la importancia que se desarrolló de la temática lo cual permiten la funcionalidad de la red informática de la universidad señor de sipan

VII. RECOMENDACIONES

Se recomienda realizar anualmente una auditoria para ver el estado actual de los equipos y su funcionamiento para que brinden un correcto servicio y que no estén vulnerables a los daños físicos como lógicos y lograr tener un control de la seguridad de su base de datos de la red informática de la red de la universidad señor de sipán.

Se recomienda tener un control de las vulnerabilidades que se encontraron en este estudio con mayor porcentaje de riesgo detectadas como: la caída del sistema por agotamiento de recursos que es muy frecuente en los sistemas de comunicación y la creación de políticas de seguridad para lograr un buen funcionamiento de la red informática señor de sipan.

Se recomienda realizar mantenimiento permanente a los diferentes equipos físicos como lógicos, ya que las vulnerabilidades son constantes y cambiantes al pasar el tiempo teniendo en cuenta que las salvaguardas no son iguales para todos los activos, además la creación de backup con nuevas políticas de seguridad y un sistema en caso de desastres naturales o robo.

VIII. REFERENCIAS BIBLIOGRAFICAS

Campos Muños, A. E., & Rios Damian, C. A. (2016). Auditoría en el uso de tecnología de información para optimizar la seguridad de la caja sipán s.a. lambayeque.

fukumoto, j. l. (2017). sistema web para la mejora en el tiempo de respuesta de reclamaciones de clientes hacia proveedores,y auditoria en planta agroindustrial de Green Perú s.a. Trujillo.

Germain, C. d. (12 de 04 de 2017). Networking and Internet Technologies. Obtenido de http://blogs.salleurl.edu/networking-and-internet-technologies/auditoria-de-seguridad-informatica/

Gómez Ramírez, V. M. (2014). Evaluación de la seguridad de la información con la metodología Octave.

Gómez Ramírez, V. M. (06 de 06 de 2014). Evaluación de la seguridad de la información con la metodología Octave. Obtenido de https://es.wikipedia.org/wiki/Auditor%C3%ADa_inform%C3%A1tica

Informática, a. (s.f.). Glosario de auditoria de sistemas. Obtenido de https://chaui201511701024029.wordpress.com/2015/05/06/glosario-auditoria-de-sistemas/

ISOTools. (2018). Caso de éxito grupo ramos. Obtenido de https://www.isotools.org/casos-de-exito/grupo-ramos-automatizacion-sistema-gestion-calidad-iso-9001-sector-venta-detalle/

Larrea Bustos, A. L., & Yangua Jumbo, B. E. (2014). Auditoría Informática y su Incidencia en los Riesgos para el manejo de la Información en la Cooperativa de Ahorro y Crédito Educadores de Tungurahua. Ambato: Universidad Técnica de Ambato. Facultad de Ingeniería en Sistemas, Electrónica e Industrial. Obtenido de http://repositorio.uta.edu.ec/jspui/handle/123456789/8099

Lucero Gómez, A. J. (2012). Análisis y gestión de riesgos utilizando la metodología Magerit. Cuenca : universidad de cuenca .

Luis Vilanova. (6 de 04 de 2017). Obtenido de https://luisvilanova.es/caso-de-exito-de-evolucion-hacia-la-empresa-digital/

MAGERIT -- versión 3.0.Libro Libro I: Método públicas, Gobierno de España-Ministerio De Hacienda y Relaciones. (2012).

Moisés, C. d. (2017). Auditoria informática para el área de gestión de créditos del banco financiero -oficina Chimbote. chimbote.

PILAR. (s.f.). manual de usuario pilar .

Ruiz Banda, J. B., & Acosta Jordán, M. G. (2016). Auditoría informática para la optimización del funcionamiento del de los sistemas informáticos de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial. Ambato: Universidad Técnica de Ambato. Facultad de Ingeniería en Sistemas, Electrónica e Industrial. Carrera de Ingeniería en Sistemas Computacionales e Informáticos.

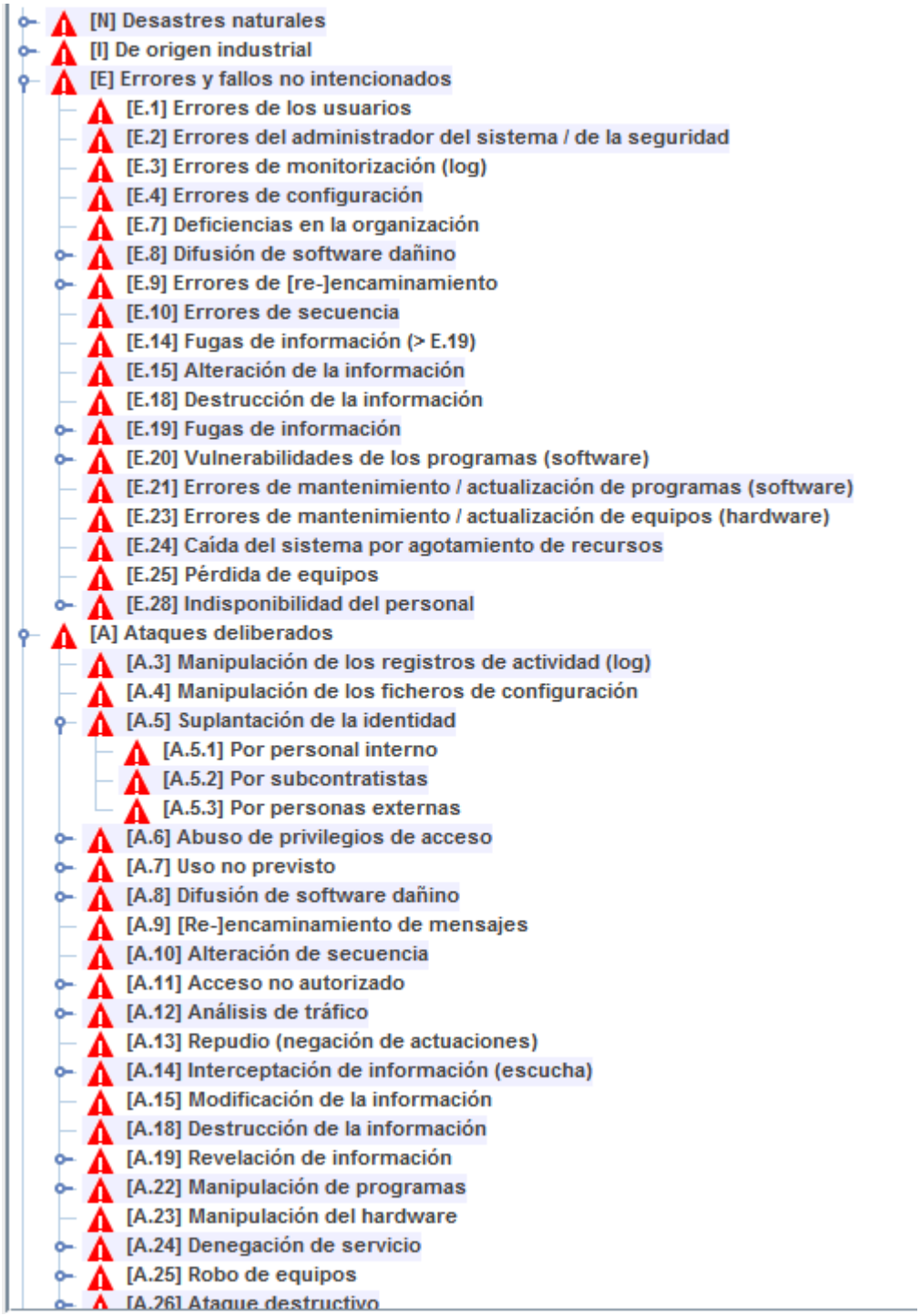
Seguridad Informática Isidro. (s.f.). Obtenido de https://sites.google.com/site/seguridadinformaticaisidro/seguridad-en-redes-inalambricas/auditoria-de-seguridad-en-red

Ulloa Barrera, J. G. (2017). Auditoría informática aplicando la metodología COBIT en el Gobierno Autónomo. Ambato: Universidad Técnica de Ambato. Facultad de Ingeniería en Sistemas, Electrónica e Industrial. Carrera Ingeniería en Sistemas Computacionales e Informáticos.

Vi3informatica. (2018). Obtenido de http://vi3informatica.es/servicios-it/casos-de-exito/

IX. ANEXOS

Lista de amenazas



Encuesta 01

Aplicada a los Colaboradores de la Universidad Señor de Sipan.

Objetivo Caracterizar las vulnerabilidades de la red informática de la Universidad Señor de Sipan.

1.- ¿Cómo califica usted el servicio brindado por parte del área de la red informática?

Excelente ( ) Bueno (x) Regular ( ) Malo ( )

2.- ¿Está usted de acuerdo con la atención brindada por parte se servicio técnico?

SI (x) No ( )

3.- ¿Con qué periodo se les da mantenimiento a las computadoras de su área?

Mensualmente (x) Semestralmente ( ) Anualmente ( )

4.- ¿Considera usted que el servicio de internet es importante al momento de laborar?

SI (x) No ( )

5.- ¿Cómo califica usted el servicio de internet?

Excelente ( ) Bueno (x) Regular ( ) Malo ( )

6.- ¿Tiene usted restricciones para ingresar a algún sitio web?

SI (x) No ( )

7.- ¿Sufre usted de constantes caídas en el servicio de internet?

SI ( ) No (x)

8.- ¿Cuál es el mayor problema que tiene al realizar su trabajo?

Cuando se va el internet y no puedo realizar mis labores o a veces cuando se Cuelgan Las computadoras y no se puede hacer nada y se pierde la información

Entrevista 01

Aplicada al responsable de la Red Informática de la Universidad de Sipan

¿Existe un método para la autenticación de usuarios que acceden a la red de datos?

¿Existen políticas para la administración de usuarios (creación y eliminación)?

¿Existen políticas para compartir información?

¿Cuenta con políticas que especifique como proceder cuando un usuario necesita acceder a información compartida?

¿Tienen políticas de respaldo?

¿Cuentan con plan de contingencia y recuperación de desastres?

¿Existe restricción de acceso a la información compartida (permisos lectura/escritura)?.

¿Cuántos computadores tienen contraseña?

¿Cuántos equipos tienen contraseña en blanco?

¿Cuántos equipos tienen contraseña relacionada con la información del usuario (identificación, nombre, apellido, nombre de hijo(a))?

¿Cuántos equipos cuentan con regulador de voltaje/UPS?

¿Cuántos servidores se encuentran protegidos por UPS?

¿Cuántos equipos tienen seguridades para evitar robo?

data center:


exinda