METODOLOGÍA PARA IDENTIFICACIÓN Y VALORACIÓN DE RIESGOS Y SALVAGUARDAS EN UNA MESA DE AYUDA TECNOLÓGICA

JEISON NICOLAS RUGE PINZON

UNIVERSIDAD PILOTO DE COLOMBIA
FACULTAD DE INGENIERÍA
PROGRAMA DE ESPECIALIZACIÓN DE SEGURIDAD INFORMÁTICA
BOGOTÁ D.C.
2011

METODOLOGÍA PARA IDENTIFICACIÓN Y VALORACIÓN DE RIESGOS Y SALVAGUARDAS EN UNA MESA DE AYUDA TECNOLÓGICA

JEISON NICOLÁS RUGE PINZÓN

Trabajo de grado para optar al título de
ESPECIALISTA EN SEGURIDAD INFORMÁTICA

Asesor
RICHARD GARCIA

UNIVERSIDAD PILOTO DE COLOMBIA
FACULTAD DE INGENIERÍA
PROGRAMA DE ESPECIALIZACIÓN DE SEGURIDAD INFORMÁTICA
IV COHORTE
BOGOTÁ D.C.
2012

Nota de Aceptación

_____
_____
_____
_____
_____
_____

_____
Firma del Presidente del Jurado

_____
Firma del Jurado

_____
Firma del Jurado

Bogotá, D.C. Febrero de 2013

A mis padres, mi hermana y mi esposa,
su apoyo siempre ha sido incondicional.

AGRADECIMIENTOS

Agradezco a Dios por permitirme y darme la posibilidad de retomar mis estudios, a mis padres porque siempre me han ayudado de muchas formas para que yo cumpla mis metas y propósitos, a mi esposa porque de ella nació una idea y me ayudo a materializarla, a mi asesor de grado Richard García por su acompañamiento en este trabajo.

TABLA DE CONTENIDO

pág.

AGRADECIMIENTOS 5
TABLA DE CONTENIDO 6
LISTA DE FIGURAS 8
LISTA DE TABLAS 9
RESUMEN 10
INTRODUCCIÓN 11
1. GENERALIDADES 12
1.1. TITULO Y LINEA DE INVESTIGACIÓN 12
1.1.1. LINEA DE INVESTIGACIÓN 12
1.2. PLANTEAMIENTO DEL PROBLEMA 12
1.3. OBJETIVOS 13
1.3.1. OBJETIVO GENERAL 13
1.3.2. OBJETIVOS ESPECIFICOS 13
1.4. JUSTIFICACIÓN 13
1.5. ALCANCE Y DELIMITACION 14
1.5.1. DELIMITACIÓN 14
1.6. MARCO TEORICO 14
1.6.1. ANTECEDENTES. 14
1.6.2. MESA DE AYUDA. 15
2. DISEÑO METODOLOGICO 17
2.1. TIPO DE INVESTIGACION 17
2.2. PROBLEMA DE ESTUDIO 18
2.3. FASES DE LA INVESTIGACIÓN. 18
2.4. POBLACIÓN. 18
2.4.1. Muestra. 18
2.4.2. Propuesta. 18
3. DESARROLLO METODOLOGICO 19

3.1. FASE 1. DEFINICIÓN Y SELECCIÓN DE UNA METODOLOGÍA PARA EL ANÁLISIS Y TRATAMIENTO DE RIESGOS EN UNA MESA DE AYUDA 19
3.1.1. COBRA. 19
3.1.2. COBIT. 21
3.1.3. CRAMM 24
3.1.4. MAGERIT. 26
3.1.5. OCTAVE 28
3.2. TABLAS COMPARATIVAS PARA SELECCIÓN DE METODOLOGÍA. 31
3.2.1. Conclusiones de las Tablas Comparativas para selección de metodología. 35
3.2.2. Selección y justificación de la metodología de análisis de riesgos. 35
3.3. FASE 2: DESCRIPCIÓN DE LA METODOLOGÍA DE ANÁLISIS Y TRATAMIENTO DE RIESGOS 36
3.3.1. Paso 1: Identificación y valoración de activos. 36
3.3.2. Paso 2: Identificación y valoración de amenazas. 40
3.3.3. Paso 3: Determinación del riesgo. 42
3.3.4. Paso 4: Identificación y valoración de salvaguardas. 43
3.4. FASE 3: DESARROLLO DE LA METODOLOGÍA DE ANÁLISIS Y TRATAMIENTO DE RIESGOS 45
3.4.1. Identificación de Activos de la mesa de ayuda. 45
3.4.2. Valoración de activos de mesa de ayuda. 48
3.4.3. Identificación y valoración de amenazas. 51
3.4.4. Identificación y valoración del riesgo 57
3.4.5. Identificación y valoración de salvaguardas. 64
CONCLUSIONES 72
RESULTADOS 74
BIBLIOGRAFÍA 76
GLOSARIO 79

LISTA DE FIGURAS

pág.

Figura 1. Componentes de Cobit. 22

Figura 2. Fases definidas en el proceso PO9. 23

Figura 3. Fases de la metodología MAGERIT 27

Figura 4. Escala de valoración de activos 38

Figura 5. Proceso de Mesa de ayuda. 46

LISTA DE TABLAS

pág.

Tabla1. Tabla comparativa por tipo de análisis. 32

Tabla2. Tabla comparativa por elementos de la metodología. 33

Tabla3. Tabla comparativa por objetivos de seguridad. 34

Tabla 4. Tabla de criterios de valoración de activos de mesa de ayuda. 38

Tabla 5. Tabla de clasificación de valoración de activos en escala de colores. ... **¡Error! Marcador no definido.**

Tabla 6. Tabla de valoración de frecuencia y degradación o impacto. 42

Tabla 7. Tabla Escala de valoración de Riesgos. 43

Tabla 8. Tabla de valoración de Salvaguardas 45

Tabla 9. Tabla de identificación de activos de mesa de ayuda. 47

Tabla 10. Tabla de valoración de activos de mesa de ayuda. 50

Tabla 11. Tabla de identificación y valoración de amenazas. 54

Tabla 12. Tabla de identificación y valoración de amenazas. 58

Tabla 13. Tabla de identificación y valoración de salvaguardas y riesgo residual. 65

RESUMEN

Las organizaciones financieras tienen implementada una mesa de ayuda tecnológica que es la encargada de la atención de las solicitudes o servicios relacionados con los activos de información tecnológicos, siendo un proceso necesario e importante para la organización se hace necesario mostrar una metodología que permita identificar y valorar los riesgos y salvaguardas que se asocian al proceso y que servirá como una guía o serie de pasos para las organizaciones en la implementación de mesas de ayuda o la revisión de una que ya esté implementada.

Para la identificación de la metodología que se aplico al proceso de mesa de ayuda, se decidió realizar una serie de tablas decomparación entre algunas metodologías de análisis de riesgos como son COBRA, COBIT, CRAMM, MAGERIT y OCTAVE; esta comparación arrojo como resultado que la metodología para la identificación y valoración de riesgos y salvaguardas de una mesa de ayuda es MAGERIT.

La metodología de MAGERIT define una metodología que se explica y en la que se aplican cuatro pasos como son la Identificación y valoración de activos, la Identificación y valoración de amenazas., la determinación del riesgo y la identificación y valoración de salvaguardas. El análisis de la mesa de ayuda en cada uno de estos pasos permite identificar factores y criterios se deben tener en cuenta para identificar y valorar los riesgos y salvaguardas que se presentan en el proceso que comprende a la mesa de ayuda tecnológica.

INTRODUCCIÓN

Los procesos que existen en cada una de las organizaciones deben ser monitoreados porque sobre cada uno de estos existen riesgos que pueden afectar su objetivo. Desde el punto de vista de la seguridad informática, los riesgos que afectan a los procesos están relacionados con los activos de información que intervienen en cada uno de los mismos; es por esta razón que se deben identificar y valorar las amenazas, riesgos y salvaguardas que envuelven a cada activo.

La mesa de ayuda tecnológica realiza el soporte para solucionar problemas técnicos a nivel de sistemas y tecnología, esto lo hace con la ayuda de software, hardware y recurso humano; elementos que requieren estar en continuo funcionamiento para que el objetivo de la mesa de ayuda se cumpla y es importante que este proceso al ser implementado o durante su funcionamiento sea revisado, valorado y analizado mediante una metodología directa que se aplique al proceso.

Debido a lo anterior se realizó un proyecto en el que se identifica una metodología que sirva como guía o base, y que muestre que factores y criterios se deben tener en cuenta para identificar y valorar los riesgos y salvaguardas que se presentan en el proceso que comprende a la mesa de ayuda tecnológica

1. GENERALIDADES

1.1. TITULO Y LINEA DE INVESTIGACIÓN

Metodología para identificación y valoración de riesgos y salvaguardas en una mesa de ayuda tecnológica.

1.1.1. LINEA DE INVESTIGACIÓN

Gestión de la seguridad y el riesgo.

1.2. PLANTEAMIENTO DEL PROBLEMA

Las organizaciones manejan dentro del departamento de tecnología un soporte de primera línea que realiza la recepción, gestión y atención de los diferentes problemas técnicos a nivel de tecnología y sistemas que se presentan durante la jornada laboral; este soporte lo realiza la mesa de ayuda y es de mucha importancia, porque al dar una solución rápida y efectiva a un problema que se presenta en cualquier área, permite que la organización cumpla sus objetivos y no falle con compromisos adquiridos con clientes.

Según este punto de vista el proceso que realiza la mesa de ayuda es vital y requiere que esté totalmente disponible para los usuarios de la organización; por esto las herramientas y activos de información de los que dependen los analistas de la mesa de ayuda deben estar dentro de un plan de tratamiento de riesgos para que no se vean afectadas en algún momento de la operación, es decir que no vallan a dejar de funcionar o a dañar por no haber tomado acciones preventivas.

Pero, ¿Qué pasaría si estos elementos de ayuda y soporte fallan?; ¿Se han identificado y valorado los riesgos que comprometen la labor diaria de la mesa de ayuda?, ¿Sera que la organización ha definido las salvaguardas correctas para mitigar los riesgos que pueden estar presentes en una mesa de ayuda?

Estas preguntas son muy importantes de analizar y responder, ya que su respuesta permitirá saber si la organización ha establecido y está aplicando una metodología con los criterios, procedimientos y controles necesarios para certificar que la confiabilidad, integridad y disponibilidad de los elementos que componen la mesa de ayuda y de todo el proceso no van a afectar y comprometer la atención a los usuarios de las áreas de la organización.

1.3. OBJETIVOS

1.3.1. OBJETIVO GENERAL.

Identificar y valorar los riesgos y salvaguardas que se presentan en el proceso que comprende a la mesa de ayuda tecnológica de una empresa del sector financiero.

1.3.2. OBJETIVOS ESPECIFICOS

- Definir una metodología para la identificación y valoración de activos de información.

- Identificar y valorar los activos de información que están involucrados en el proceso de atención de una mesa de ayuda de una empresa del sector financiero.

- Definir la metodología para la identificación y valoración de los riesgos que se presentan en el proceso de una mesa de ayuda tecnológica.

- Generar conclusiones y resultados que se puedan tener en cuenta en el momento de implementar una mesa de ayuda teniendo en cuenta niveles de seguridad apropiados.

1.4. JUSTIFICACIÓN

Cuando un área o una empresa dependen de herramientas tecnológicas para cumplir con su objetivo principal, automáticamente debe implementar un proceso para dar atención y soporte a estas herramientas. Si este proceso se implementa en forma de una mesa de ayuda tecnológica, esta mesa también debe mantenerse funcionando con total disponibilidad; y para lograr esto se requiere una metodología en la que sean identificados los riesgos que la pueden afectar y que lleven a detener su funcionamiento ante los usuarios de las demás áreas.

Como se ve es de gran importancia que el proceso de soporte de la mesa de ayuda funcione aún mejor que las áreas que atiende, para que así su servicio sea rápido, confiable y óptimo. Dado este caso y como ya se mencionó, un punto crucial y necesario es realizar una metodología en la que se definan criterios para la identificación y valoración de riesgos que afectan a la mesa de ayuda. Este documento es un análisis básico que puede servir de guía para el área de tecnología de las organizaciones que deseen implementar una mesa de ayuda o que ya esté en funcionamiento.

1.5. ALCANCE Y DELIMITACION

El presente proyecto pretende dar a conocer las amenazas, riesgos y salvaguardas que se presentan en el proceso que comprende a la mesa de ayuda tecnológica de una empresa del sector financiero. Para desarrollar este objetivo se realizaran las siguientes actividades:

- Identificar los activos de información que están involucrados en el proceso de la mesa de ayuda tecnológica.

- Identificar los riesgos que se presentan en el proceso de la mesa de ayuda tecnológica.

- Generación de conclusiones y resultados.

1.5.1. DELIMITACIÓN

Las características de la mesa de ayuda que se tendrán en cuenta para este proyecto son las siguientes:

- La mesa de ayuda que se analizará en el transcurso del trabajo está basada en la mesa de ayuda tecnológica de una entidad financiera como lo es un banco.

- Mesa de ayuda integrada por analistas los cuales atienden solicitudes de problemas tecnológicos de una organización financiera como lo es un banco, estas solicitudes conocidas como tickets o servicios se reciben por medio de una herramienta web o por medio de llamada telefónica. La mesa de ayuda puede ser un área directa de la organización o un área que hace parte de un outsourcing que presta el servicio.

- Las instalaciones donde la mesa de ayuda realiza sus funciones pueden ser de la organización o propias del outsourcing si es el caso.

1.6. MARCO TEORICO

1.6.1. ANTECEDENTES.

Con el avance de la tecnología, las organizaciones empezaron a cambiar las herramientas de trabajo de sus empleados, se pasó de utilizar elementos como máquinas de escribir a computadores de escritorio por solo dar un ejemplo del caso. La modernización tecnológica hizo que las compañías crearan dentro de su estructura organizativa el área de Tecnología y Sistemas o similar; esta área que

es la encargada de administrar, soportar e implementar el software, hardware, sistemas de comunicación y demás, a su vez requirió crear un departamento el cual se encargara de dar atención de primera mano a los problemas e incidentes que se relacionan con la parte tecnológica, a este departamento dentro del área de tecnología se le llamó mesa de ayuda. Debido a la relación de los objetivos de este proyecto con esta área o proceso, a continuación se define que es una mesa de ayuda y cuáles son sus funciones.

1.6.2. MESA DE AYUDA.

La mesa de ayudaque también es conocida dentro del ambiente empresarial como Help Desk, mesa de Servicio o service Desk,es la unión de varios servicios que permiten dar gestión y solucionan los incidentes relacionados con las TICs (Tecnologías de la información y comunicaciones) que le suceden a un empleado de la organización.

Existen dos propósitosque debe cumplirla mesa de ayuda, el primero es resolver cualquier problema que tengan los usuarios con el sistema así como ayudarlos a utilizarlo de una manera óptima. En algunas organizaciones también es la encargada de brindarles acceso al sistema a los usuarios asignando usuarios y contraseñas. Las funciones de la mesa de ayuda pueden ser atendidas por personal contratado de manera directa por la organización o a través de un proveedor externo u outsourcing; para que una mesa de ayuda sea efectiva y optima es necesario que cuente con personal que tenga las habilidades y conocimientos técnicos necesarios para ofrecer ayuda de manera rápida y eficaz. Cabe aclarar que existen casos en que la mesa de ayuda puede solucionar un problema o incidente de manera inmediata o asignar y escalar el servicio a personal con las capacidades y disponibilidad que se requieran para el caso.

La mesa de ayuda establecerá una estructura que debe ser diseñada con el cliente ya que al mismo le permitirá saber cuál es el manejo de los servicios, su clasificación y gestión de acuerdo a su prioridad. Para que la función de la mesa de ayuda mejore cada día más, esta debe llevar un registro del tipo, número de solicitudes y el tiempo en que dio solución al servicio, con esto identificara en que se deben mejorar las capacitaciones y procedimientos. A continuación otras actividades que realiza la mesa de ayuda.[1]

- Debe cumplir con todo el proceso de recibir, registrar, analizar, escalar, hacer seguimiento y dar solución a los requerimientos de servicios solicitados por los usuarios.

[1]Mesa de ayuda. [on line]. [Fecha de consulta: 10 de Noviembre de 2011]. Disponible en http://aceproject.org/main/espanol/et/etd04e.htm

- Cuando un usuario lo solicite debe informarle sobre el estado en el que se encuentra el servicio.

- Estar en la capacidad de dar el soporte técnico inicial al usuario.

- Tener la capacitación para asesorar a los usuarios en la correcta utilización de la infraestructura, hardware y software.

- Aplicar los procedimientos de instalación de software que tiene establecido el cliente.

- Si el servicio lo requiere debe realizar la asignación del mismo a otras áreas funcionales para su solución.

- Si la mesa de ayuda tiene herramientas para resolver por vía control remoto un servicio debe intentarlo en forma inmediata.

- Realizar auditoria permanentemente de los servicios que ha solucionado.

- Mantener informes de reportes y estadísticas según niveles de servicio, así como de los servicios creados para la identificación de servicios.

- Llevar un control de tiempos de respuesta y escalamiento de los servicios en caso de no cumplirlos.

- Realizar el reporte de cumplimiento de niveles de servicio de manera periódica.

2. DISEÑO METODOLOGICO

2.1. TIPO DE INVESTIGACION

El método de investigación que se utilizará en el presente proyecto es un método de tipo inductivo – descriptivo.

El método inductivo o inductivismo es un método científico que obtiene conclusiones generales a partir de premisas particulares. Se trata del método científico más usual, que se caracteriza por cuatro etapas básicas: la observación y el registro de todos los hechos: el análisis y la clasificación de los hechos; la derivación inductiva de una generalización a partir de los hechos; y la contrastación.[2]

El estudio de tipo descriptivo es utilizado básicamente para:

- Describir (medir) situaciones, eventos o fenómenos.
- Buscan especificar las propiedades importantes de personas, grupos, comunidades o cualquier otro fenómeno.
- Se selecciona una serie de variables o cuestiones y se miden cada una de ellas independientemente para luego puntualizar lo que se estudia.
- Puede ofrecer algunas posibilidades rudimentarias de predicción o sugerir algunas inferencias.
- En comparación con la naturaleza poco estructurada de los estudios exploratorios (centrados en descubrir) requiere un buen conocimiento acerca del problema para formular preguntas específicas que busca responder.[3]

[2]Definición de método inductivo.[on line]. [Fecha de consulta: 10 de Noviembre de 2011]. Disponible en http://definicion.de/metodo-inductivo/

[3]LACHEROS, Yanet Mejia.Investigación I. Colombia: Especialización en seguridad informática, 2010 42 p.

2.2. PROBLEMA DE ESTUDIO.

Activos y riesgos en una mesa de ayuda tecnológica.

2.3. FASES DE LA INVESTIGACIÓN.

Las fases que se llevaran a cabo para dar cumplimiento con los objetivos son las siguientes.

Fase 1: Definición y selección de una metodología para el análisis y tratamiento de riesgos en una mesa de ayuda

Fase 2: Descripción de la metodología de análisis y tratamiento de riesgos.

Fase 3: Desarrollo de la metodología de análisis y tratamiento de riesgos

Fase 4: Muestra de conclusiones y resultados que se puedan tener en cuenta en el momento de implementar una mesa de ayuda teniendo en cuenta niveles de seguridad apropiados.

2.4. POBLACIÓN.

Este proyecto se realiza basándose en una mesa de ayuda tecnológica que es prestada por una empresa de outsourcing a una empresa financiera.

2.4.1. Muestra.

1 Mesa de ayuda tecnológica que cumple con el alcance y delimitación.

2.4.2. Propuesta.

La identificación y valoración de activos de información y riesgos que se presentan en una mesa de ayuda tecnológica mediante una metodología aplicada permite generar conclusiones y resultados que servirán para la implementación de nuevas mesas de ayuda y la revisión de las que ya están en funcionamiento.

3. DESARROLLO METODOLOGICO

3.1. FASE 1. DEFINICIÓN Y SELECCIÓN DE UNA METODOLOGÍA PARA EL ANÁLISIS Y TRATAMIENTO DE RIESGOS EN UNA MESA DE AYUDA

Como ya se ha definido y contextualizado que es una mesa de ayuda, ahora se procederá a conocer y explicar diferentes tipos de metodologías y herramientas que existen para identificar, analizar y tratar riesgos.

Una metodología es una guía de pasos que se deben seguir para realizar las acciones propias de una investigación, en la metodología se indica que hacer y cómo actuar cuando se quiere obtener algún tipo de investigación. Una metodología es aquel enfoque que permite observar un problema de una forma total, sistemática y disciplinada. Una metodología de tratamiento riesgos es una guía que permitirá identificar los riesgos en un proceso y su respectivo tratamiento de acuerdo a su complejidad.

Una metodología no es lo mismo que una técnica de investigación, las técnicas son parte de una metodología y se definen como aquellos procedimientos que se utilizan para llevar a cabo la metodología. Las herramientas son aplicaciones que ayudan a recoger los datos de manera organizada y entregan resultados que se pueden aprovechar en las metodologías para su análisis.[4]

Para escoger la metodología que se utilizará para el tratamiento de riesgos de una mesa de ayuda, se explicarán y compararan cinco metodologías: COBRA, COBIT, CRAMM, MAGERIT y OCTAVE.

3.1.1. COBRA.

Es una metodología que consiste en una serie de análisis de riesgos para consulta y herramientas de revisión de seguridad. La sigla COBRA significa Consultative, objective and Bi-functionalRiskAnalysis, está metodología se desarrolló reconociendo la naturaleza cambiante de las TI y su seguridad, y las exigencias por las empresas en mejorar en cada una de estas áreas.

La primera causa que llevo a desarrollar esta metodología fue el creciente reconocimiento de que la seguridad de TI es ununun tema de negocios, convirtiendo en gran medida el pensamiento de que las revisiones de seguridad deben ser un negocio relacionado con soluciones de costo y recomendaciones justificadas. Otra causa es que a finales de los años 90, muchas organizaciones buscaron un mejor

[4] ¿Qué es una metodología?[on line]. [Fecha de consulta: 10 de Noviembre de 2011]. Disponible en http://www.misrespuestas.com/que-es-una-metodologia.html

rendimiento y que fuera más visible en sus presupuestos de seguridad. Para alcanzar esto, se debían adoptar nuevos enfoques a las limitaciones de experiencia, tiempo y dinero.

A menudo, una técnica de análisis de riesgo se emplea, sin embargo los métodos y herramientas convencionales simplemente no responden a las nuevas exigencias de la gestión empresarial. COBRA en su metodología hace frente a estas cuestiones de manera adecuada.

La metodología COBRA se desarrolló en completa cooperación con una de las principales instituciones financieras del mundo y después de muchos años de investigación. Se reconoció que todos los empleados deben participar desde el principio porque esto conlleva a una serie de ventajas en las formas de revisión. El resultado fue una metodología de análisis de riesgos en las que se cumplen exigentes necesidades y se satisfacen plenamente las demandas cambiantes en la seguridad y equipos auditores.

Proporciona un completo servicio de análisis de riesgos compatibles con las metodologías más reconocidas (cualitativas y cuantitativas). Se trata de un sistema de cuestionarios basados en usuarios expertos en sistemas y una amplia base de conocimientos. COBRA evalúa la importancia relativa de todas las amenazas y vulnerabilidades y genera recomendaciones y soluciones adecuadas. Además, sus informes proporcionan una evaluación escrita del puntaje de riesgo relativo, o nivel para cada categoría de riesgo. Los riesgos identificados son automáticamente vinculados con las posibles consecuencias que pueden ser pérdidas financieras, pérdidas de clientes y demás pérdidas económicas o de negocio para la empresa o departamento

Flexibilidad: Una gran ventaja es la modularización de la base de datos de COBRA. Esto permite al módulo de preguntas estar dirigido a personal que tiene el conocimiento del tema apropiado. Para nuevos desarrollos la flexibilidad también permite una evaluación etapa por etapa (diseño, desarrollo, pruebas de aceptación y puesta en práctica). Además de aumentar la precisión este enfoque permite tener en cuenta más detalles que garantizan mejores resultados y soluciones.

Personalización automática: Como no hay dos empresas que sean iguales, tampoco lo son sus requisitos de seguridad; por lo tanto COBRA va a generar cuestionarios preestablecidos en la base de datos que específicamente se adaptan a la organización, al medio ambiente y el sistema de evaluación. Esta función se realiza dinámicamente a medida que las preguntas se responden y COBRA obtiene más información.

Auto análisis: El consultor de riesgos COBRA está diseñado para ser auto analítico. Esto permite que se use sin la necesidad de un conocimiento detallado

de seguridad o la experiencia en el uso de un software de gestión de riesgos. Tampoco hay necesidad de contratar a costosos consultores para realizar copias de seguridad del sistema.

Pruebas de solución: Las pruebas de hipótesis están totalmente soportadas. El impacto que los controles específicos adicionales pueden tener sobre el nivel de riesgos de un sistema puede ser comprobado de forma dinámica. Por lo tanto se establece rápidamente la solución más rentable para las exposiciones individuales.

Reportes: Los informes elaborados por COBRA no son una salida estándar. Son informes de profesionales de negocio y son adecuados para la interpretación de parte técnica e informal. Amplios formatos de reportes están disponibles, y para máxima flexibilidad todas las secciones son opcionales. Además el reporte puede ser impreso, o enviado a un archivo.[5]

3.1.2. COBIT.

Objetivos de Control para Información y Tecnologías Relacionadas. COBIT es una metodología aceptada mundialmente para el adecuado control de proyectos de tecnología, los flujos de información y los riesgos que éstas implican. La metodología se utiliza para planear, implementar, controlar y evaluar el gobierno sobre TIC; incorporando objetivos de control, directivas de auditoría, medidas de rendimiento y resultados, factores críticos de éxito y modelos de madurez.

Cobit permite el desarrollo de una política clara y una buena práctica para el control TI en las organizaciones. COBIT acentúa el cumplimiento regulatorio, ayuda a las organizaciones a aumentar el valor asociado al área de TI, habilita la alineación y simplifica la puesta en práctica del marco de referencia COBIT.[6]

COBIT da soporte al gobierno de TI al brindar un marco de trabajo que garantiza que:

- TI está alineada con el negocio.
- TI capacita el negocio y maximiza los beneficios.
- Los recursos de TI se usen de manera responsable.

---

[5] IntroductiontoCOBRA[on line].[Fecha de consulta: 10 de Noviembre de 2011]. Disponible en http://www.security-risk-analysis.com/introcob.htm

[6] COBIT.ControlOBjectivesforInformation and relatedTechnology.ISACA [on line].Bogotá. Colombia [fecha de consulta: 10 de Noviembre de 2011]. Disponible en www.isaca-bogota.net/metodologias/cobit.aspx

- Los riesgos de TI se administren apropiadamente.

Áreas focales del gobierno de TI:

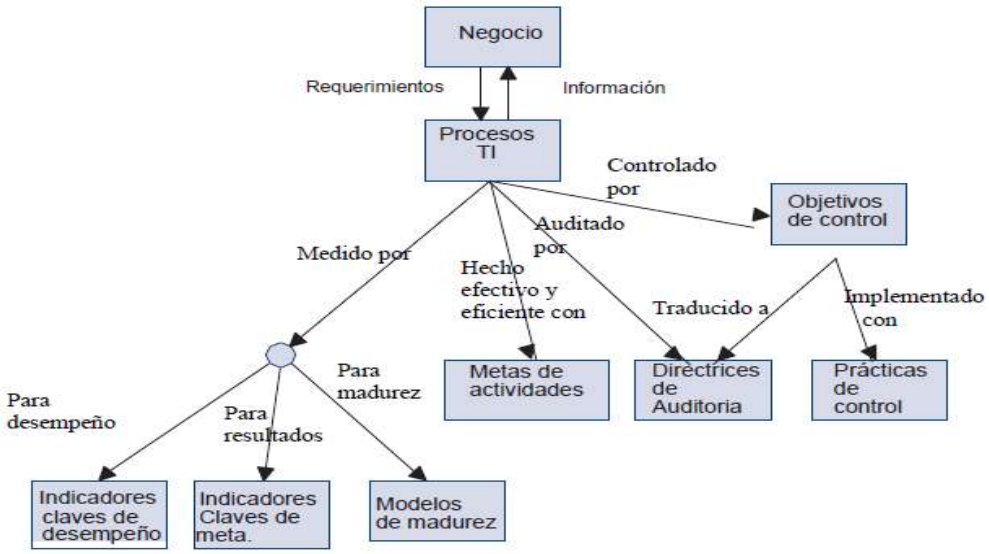
- Alineación estratégica se enfoca en garantizar el vínculo entre los planes de negocio y de TI; en definir, mantener y validar la propuesta de valor de TI; y en alinear las operaciones de TI con las operaciones de la empresa.

- Generación de valor se refiere a ejecutar la propuesta de valor a lo largo del ciclo de entrega, asegurando que TI genere los beneficios prometidos en la estrategia, concentrándose en optimizar los costes y en proporcionar el valor intrínseco de la TI.

- Gestión de recursos trata de la inversión óptima, así como la administración adecuada de los recursos críticos de TI: aplicaciones, información, infraestructura y personas. Los temas clave se refieren a la optimización de conocimiento y de infraestructura.

- Gestión de riesgos requiere conciencia de los riesgos por parte de los altos ejecutivos de la empresa, un claro entendimiento del apetito de riesgo que tiene la empresa, comprender los requerimientos de cumplimiento, transparencia de los riesgos significativos para la empresa, y la inclusión de las responsabilidades de gestión de riesgos dentro de la organización.

Figura 1. Componentes deCobit.



Fuente: Resumen ejecutivo Cobit 4.0[7]

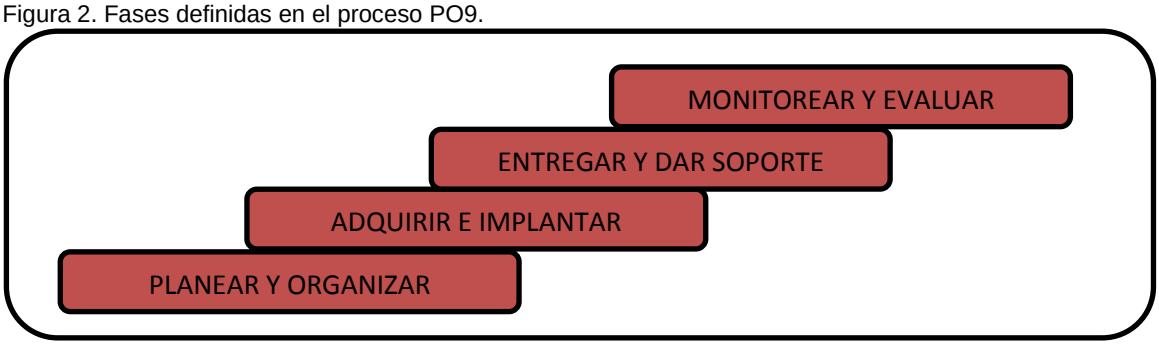
[7]COBIT 4.1.Control OBjectives for Information and related Technology.Resumenejecutivo.ISACA [on line].Bogotá. Colombia [fecha de consulta: 10 de Junio de 2011]. Disponible en www.isaca-bogota.net/metodologias/cobit.aspx

Cobit define 10 procesos:

- PO1 Definir un plan estratégico de TI
- PO2 Definir la arquitectura de la información
- PO3 Determinar la dirección tecnológica
- PO4 Definir los procesos, organización y relaciones de TI
- PO5 Administrar la inversión en TI
- PO6 Comunicar las aspiraciones y la dirección de la gerencia
- PO7 Administrar recursos humanos de TI
- PO8 Administrar la calidad
- PO9 Evaluar y administrar los riesgos de TI
- PO10 Administrar proyectos.

El proceso PO9 en el cual se evalúa y administra el riesgo de TI se basa en las siguientes fases:

Figura 2. Fases definidas en el proceso PO9.



Fuente: El autor

Objetivos de control detallados PO9 Evaluar y administrar los riesgos de TI

PO9.1 Alineación de la administración de riesgos de TI y del negocio Integrar el gobierno, la administración de riesgos y el marco de control de TI, al marco de trabajo de administración de riesgos de la organización. Esto incluye la alineación con el apetito de riesgo y con el nivel de tolerancia al riesgo de la organización

PO9.2 Establecimiento del contexto del riesgo Establecer el contexto en el cual el marco de trabajo de evaluación de riesgos se aplica para garantizar resultados apropiados. Esto incluye la determinación del contexto interno y externo de cada evaluación de riesgos, la meta de la evaluación y los criterios contra los cuales se evalúan los riesgos.

PO9.3 Identificación de eventos Identificar todos aquellos eventos (amenazas y vulnerabilidades) con un impacto potencial sobre las metas o las operaciones de la empresa, aspectos de negocio, regulatorios, legales, tecnológicos, de sociedad

comercial, de recursos humanos y operativos. Determinar la naturaleza del impacto – positivo, negativo o ambos – y dar mantenimiento a esta información.

PO9.4 IT Evaluación de riesgos Evaluar de forma recurrente la posibilidad e impacto de todos los riesgos identificados, usando métodos cualitativos y cuantitativos. La posibilidad e impacto asociados a los riesgos inherentes y residuales se debe determinar de forma individual, por categoría y con base en el portafolio.

PO9.5 Respuesta a los riesgos Identificar los propietarios de los riesgos y a los dueños de procesos afectados, y elaborar y mantener respuestas a los riesgos que garanticen que los controles rentables y las medidas de seguridad mitigan la exposición a los riesgos de forma continua. La respuesta a los riesgos debe identificar estrategias de riesgo tales como evitar, reducir, compartir o aceptar. Al elaborar la respuesta, considerar los costos y beneficios y seleccionar respuestas que limiten los riesgos residuales dentro de los niveles de tolerancia de riesgos definidos.
PO9.6 Mantenimiento y monitoreo de un plan de acción de riesgos Asignar prioridades y planear las actividades de control a todos los niveles para implantar las respuestas a los riesgos, identificadas como necesarias, incluyendo la identificación de costos, beneficios y la responsabilidad de la ejecución. Buscar la aprobación para las acciones recomendadas y la aceptación de cualquier riesgo residual, y asegurarse de que las acciones comprometidas son propiedad del dueño (s) de los procesos afectados. Monitorear la ejecución de los planes y reportar cualquier desviación a la alta dirección.

3.1.3. CRAMM

CCTA RiskAnalysis and Management Method.CRAMM es una metodología de análisis de riesgos desarrollada en el Reino Unido por la Agencia Central de Cómputo y Telecomunicaciones (CCTA). Comenzó a desarrollarse en la década de 1980 y actualmente está en su versión 5.1. Es el método de análisis de riesgos preferente en Organismos de la Administración Pública británica.[8] El mantenimiento y la gestión de la metodología están a cargo de la empresa privada de consultoría InsightConsulting, actualmente integrada en Siemens.

Uno de los aspectos principales de CRAMM es el soporte que proporciona la herramienta informática que la soporta, con una base de datos de:

- Más de 400 tipos de activos
- Más de 25 tipos de impacto

[8]MATALOBOS VEIGA, Juan Manuel. Análisis de riesgos de seguridad de la información. Madrid: Universidad Politécnica de Madrid. Facultad de informática, 2009. 88 p.

- 38 tipos de amenaza
- 7 tipos de medida del riesgo
- Más de 3.500 salvaguardas.

Actualmente CRAMM soporta tres tipos de revisiones:

- CRAMM Express
- CRAMM Expert
- BS7799

La metodología CRAMM define tres fases para la realización del análisis de riesgos:

Fase 1: Establecimiento de objetivos de seguridad:

- Definir el alcance del estudio.
- Definir el valor de la información entrevistando a los usuarios sobre los impactos potenciales para el negocio que podrían producirse por la indisponibilidad, destrucción, divulgación o modificación.
- Identificar y evaluar los activos físicos que forman parte del sistema.
- Identificar y evaluar los activos de software que forman parte del sistema.

Fase 2: Evaluación de riesgos:

- Identificar y valorar el tipo y nivel de las amenazas que pueden afectar al sistema.
- Valorar las vulnerabilidades de los sistemas ante las amenazas identificadas.
- Combinar las valoraciones de amenazas y vulnerabilidades para calcular la medida de los riesgos.

Fase 3: Identificación y selección de contramedidas: Los principales productos de la metodología CRAMM son:

- Documento de inicio del proyecto
- Informes de análisis de riesgos
- Informes de gestión de riesgos, basados en una base de datos de más de 3.500 salvaguardas técnicas y organizativas.

- Plan de implantación

3.1.4. MAGERIT.

En su versión 2 es una metodología de análisis y gestión de riesgos creada por el Consejo Superior de Administración Electrónica 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.

Magerit persigue los siguientes objetivos:

- Concienciar a los responsables de los sistemas de información de la existencia de riesgos y de la necesidad de detectarlos a tiempo.
- Ofrecer un método sistemático para analizar tales riesgos.
- Ayudar a descubrir y planificar las salvaguardas oportunas para mantener los riesgos bajo control.
- Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso.[9]

Esta metodología está estructurada en 3 libros o volúmenes que se describen a continuación:

- **Libro 1 – Método.** Es el libro principal con el cual se hace una introducción general a la metodología.
- **Libro 2 – Catalogo de Elementos**. Este segundo libro ofrece diversas herramientas o guías para la implementación de la metodología, está dividido en 5 partes:

    1. Tipos de Activos
    2. Dimensiones de Valoración
    3. Criterios de Valoración
    4. Amenazas
    5. Salvaguardas

[9] Portal Administración Electrónica. Centro de Transferencia de Tecnología – CTT. MAGERIT versión 2. [on line]. Madrid España.[fecha de consulta: 13 de Junio de 2011]. Disponible en http://administracionelectronica.gob.es.

- **Libro 3 – Guía de Técnicas.** Describe algunas técnicas a utilizar en las fases del análisis. Las técnicas descritas en este libro son:

  - **Técnicas específicas para el análisis de riesgos:**

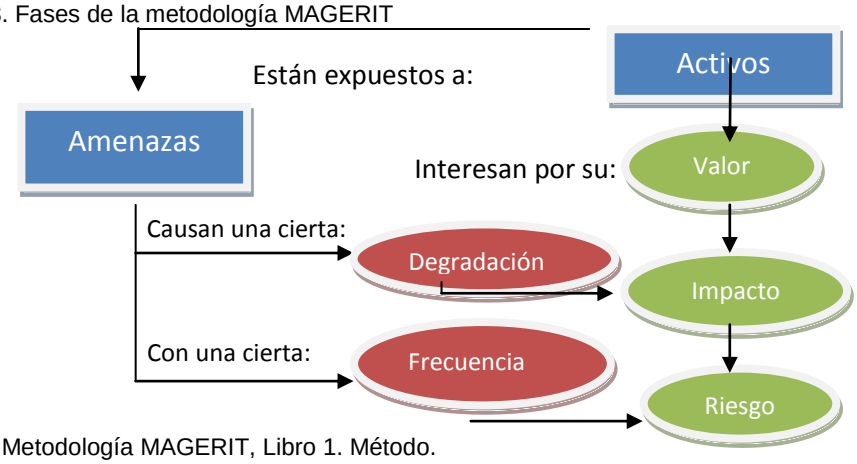
    - Análisis mediante tablas
    - Análisis Algorítmico
    - Arboles de Ataque

  - **Técnicas Generales:**

    - Diagrama de procesos
    - Técnicas graficas
    - Planificación de proyectos
    - Sesiones de trabajo
    - Valoración Delphi

Durante un análisis de riesgos, la metodología Magerit especifica ciertos pasos a seguir para su realización:

Figura 3. Fases de la metodología MAGERIT



Fuente: Metodología MAGERIT, Libro 1. Método.

En la figura anterior se puede observar la relación que existe entre las variables que intervienen en un análisis de riesgos; Un detalle a tener en cuenta es que en la metodología Magerit la palabra vulnerabilidad la cual define como: potencialidad o posibilidad de ocurrencia de una amenaza sobre un activo, no es reemplazada por el termino degradación del activo y frecuencia de ocurrencia de amenaza.

Los pasos propuestos por la metodología Magerit se definen en las siguientes actividades:

- Identificar Activos
- Identificar Salvaguardas de seguridad existentes

- Valorar los activos
- Identificar Amenazas
- Valorar Amenazas
- Identificar vulnerabilidades
- Estimar vulnerabilidades
- Identificar Impacto
- Valorar impactos
- Evaluar el riesgo intrínseco
- Evaluar el riesgo efectivo

3.1.5. OCTAVE

Operationally Critical Threat, Asset and Vulnerability Evaluation.OCTAVE es un modelo para la creación de metodologías de análisis de riesgos desarrollado por la Universidad de Carnegie Mellon.[10] Es una evaluación de riesgos estratégica y técnica de seguridad. OCTAVE es auto-dirigido, lo que significa que el personal vinculado debe asumir la responsabilidad de llevar a cabo su implementación dentro de la organización.

La técnica aprovecha el conocimiento de los relacionados con los procesos para terminar el estado de seguridad actual dentro de la organización.

Cualquier metodología que aplique los criterios puede considerarse compatible con el modelo OCTAVE. Las tres metodologías publicadas a la fecha son:

- ✓ **OCTAVE**: La metodología original, definida para grandes organizaciones.
- ✓ **OCTAVE-S**: Metodología definida para pequeñas organizaciones.
- ✓ **OCTAVE Allegro**: Metodología definida para analizar riesgos con un mayor enfoque en los activos de información, en oposición al enfoque en los recursos de información.

Los criterios que forman el núcleo de OCTAVE son:

- La metodología debe ser auto-dirigida:
  - RA.1 Equipo de análisis
  - RA.2 Capacidades del equipo de análisis

[10]OCTAVE Method Implementation Guide.Carnegie Mellon University [on line].Pittsburgh Pensilvania.[fecha de consulta: 9 de Junio de 2011]. Disponible en www.cert.org/octave/octavemethod.html

- Las medidas deben ser adaptables a las necesidades:
    - RA.3 Catálogo de prácticas
    - RA.4 Perfil genérico de amenazas
    - RA.5 Catálogo de vulnerabilidades
- El proceso debe ser definido:
    - RA.6 Actividades de evaluación definidas
    - RA.7 Documentación de los resultados de la evaluación
    - RA.8 Alcance de la evaluación
- El proceso debe ser continuo:
    - RA.9 Próximos pasos
    - RA.3 Catálogo de prácticas
- El proceso debe seguirse con visión de futuro.
    - RA.10 Enfoque en riesgos
- El proceso debe centrarse en un reducido número de riesgos críticos:
    - RA.8 Alcance de la evaluación
    - RA.11 Actividades enfocadas
- Gestión integrada:
    - RA.12 Aspectos organizativos y tecnológicos
    - RA.13 Participación de negocio y de áreas tecnológicas
    - RA.14 Participación de la alta dirección
- Comunicación abierta:
    - RA.15 Enfoque colaborativo
- Perspectiva global:
    - RA.12 Aspectos organizativos y tecnológicos
    - RA.13 Participación de negocio y de áreas tecnológicas
- Equipo de trabajo
    - RA.1 Equipo de análisis

- RA.2 Capacidades del equipo de análisis
- RA.13 Participación de negocio y de áreas tecnológicas
- RA.15 Enfoque colaborativo

Para cada metodología se define un conjunto de procesos diferente adaptado a las necesidades particulares, siempre cumpliendo todos los criterios. Los procesos de cada una de las metodologías son:

- **Fase 1: Visión organizativa**
  - RO1.1 Activos críticos
  - RO1.2 Requerimientos de seguridad para los activos críticos
  - RO1.3 Amenazas sobre los activos críticos
  - RO1.4 Prácticas de seguridad actuales
  - RO1.5 Vulnerabilidades organizativas actuales
- **Fase 2: Visión tecnológica**
  - RO2.1 Componentes clave
  - RO2.2 Vulnerabilidades tecnológicas actuales
- **Fase 3: Estrategia y desarrollo del plan**
  - RO3.1 Riesgos sobre activos críticos
  - RO3.2 Medidas contra los riesgos
  - RO3.3 Estrategia de protección
  - RO3.4 Planes de mitigación del riesgo.[11]

[11]Alberts, Christopher, *etal.*Introduction to the OCTAVE® Approach. Carnegie MellonUniversity, 2003.

3.2. TABLAS COMPARATIVAS PARA SELECCIÓN DE METODOLOGÍA.

Para la generación de las tablas de comparación que permitirán soportar la selección de la metodología; se ha decidido tener en cuenta las siguientes características.

Tipo de Análisis: En esta tabla se busca verificar si cada una de las metodologías abarca dentro de su planteamiento de análisis los métodos cuantitativo, cualitativo o mixto; valorando su aplicabilidad desde un nivel completo a un nivel en el que no tiene el tipo de análisis.
Elementos de la metodología: En esta tabla se pretende verificar si las metodologías abarcan y analizan la mayor cantidad de elementos como lo son los procesos, los activos, las dependencias, vulnerabilidades, amenazas y salvaguardas; valorando su análisis en cada uno de ellos desde un nivel completo a un nivel en el que no realizan un análisis del elemento.

Objetivos de seguridad: En esta tabla se quiere valorar que metodología abarca en una mayor proporción los objetivos de seguridad como son la confidencialidad, la integridad, la disponibilidad, la autenticidad y la trazabilidad; valorando su análisis en cada uno de los objetivos desde un nivel completo a un nivel en el que no abarcan el objetivo.

Tabla de Comparación por tipo de análisis (cuantitativo, cualitativo y mixto).

Tabla1. Tabla comparativa por tipo de análisis.

NOMBRE	TIPO DE ANALISIS			TOTAL
	CUANTITATIVO	CUALITATIVO	MIXTO	
COBRA	3,32	3,32	1,66	8,3
COBIT	6,66	6,66	4,98	18,3
CRAMM	6,66	6,66	0	13,32
MAGERIT	6,66	6,66	0	13,32
OCTAVE	3,32	3,32	3,32	9,96

Fuente: Análisis de riesgos de seguridad de la información[12]

Leyenda y equivalencia: Completo: 6,66 Amplio: 4,98 Satisfactorio: 3,32
Pobre: 1,66 No tiene: 0

[12]MATALOBOS VEIGA, Juan Manuel. Análisis de riesgos de seguridad de la información. Madrid: Universidad Politécnica de Madrid. Facultad de informática, 2009. 107 p

Tabla de Comparación por elementos de la metodología.

Tabla2. Tabla comparativa por elementos de la metodología.

NOMBRE	ELEMENTOS DE LA METODOLOGÍA							TOTAL
	PROCESOS	ACTIVOS	RECURSOS	DEPENDENCIAS	VULNERABILIDADES	AMENAZAS	SALVAGUARDAS	
COBRA	0	4,98	4,98	3,32	3,32	3,32	3,32	23.34
COBIT	6,66	6,66	6,66	6,66	6,66	6,66	6,66	46,62
CRAMM	0	6,66	0	6,66	6,66	6,66	6,66	33,3
MAGERIT	0	6,66	6,66	6,66	6,66	6,66	6,66	39,96
OCTAVE	6,66	6,66	6,66	6,66	6,66	6,66	6,66	46,62

Fuente: Análisis de riesgos de seguridad de la información[13]

Leyenda y equivalencia: Completo: 6,66 Amplio: 4,98 Satisfactorio: 3,32 Pobre: 1,66 No tiene: 0

[13]MATALOBOS VEIGA, Juan Manuel. Análisis de riesgos de seguridad de la información. Madrid: Universidad Politécnica de Madrid. Facultad de informática, 2009. 108 p

Tabla de Comparación por objetivos de seguridad

Tabla3. Tabla comparativa por objetivos de seguridad.

NOMBRE	OBJETIVOS DE SEGURIDAD					TOTAL
	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	AUTENTICIDAD	TRAZABILIDAD	
COBRA	4,98	4,98	4,98	0	0	14,94
COBIT	6,66	6,66	6,66	0	0	19,98
CRAMM	6,66	6,66	6,66	0	0	19,98
MAGERIT	6,66	6,66	6,66	6,66	6,66	33,3
OCTAVE	6,66	6,66	6,66	0	0	19,98

Fuente: Análisis de riesgos de seguridad de la información.[14]

Leyenda y equivalencia: Completo: 6,66 Amplio: 4,98 Satisfactorio: 3,32
Pobre: 1,66 No tiene: 0

[14]MATALOBOS VEIGA, Juan Manuel. Análisis de riesgos de seguridad de la información. Madrid: Universidad Politécnica de Madrid. Facultad de informática, 2009. 109 p

La sumatoria de puntajes totales por tablas de comparación dio como resultado:

COBRA = 46,48
COBIT = 84,9
CRAMM = 66,6
MAGERIT = 86,58
OCTAVE = 76,56

3.2.1. Conclusiones de las Tablas Comparativas para selección de metodología.

- ✓ COBIT es la metodología que mayor tipo de análisis cuantitativo, cualitativo y mixto ofrece.

- ✓ COBIT, OCTAVE y MAGERIT son las metodologías que ofrecen un análisis más completo de elementos dentro del proceso u organización.

- ✓ MAGERIT es la metodología que ofrece un análisis más completo desde los objetivos de seguridad.

3.2.2. Selección y justificación de la metodología de análisis de riesgos.

Para elegir la metodología de análisis de riesgos que se utilizará en el proceso de mesa de ayuda, hay que dejar claro que en este caso estamos levantando una metodología para una mesa de ayuda con unas características que se definieron en la delimitación del trabajo; estas limitaciones establecen que este trabajo se basa en una mesa de ayuda de un banco y que la administra una empresa tipo outsourcing.

Por políticas de confidencialidad de las organizaciones involucradas no se permitió el levantamiento de información del proceso por parte del personal que lo conoce, y la información levantada se obtuvo de los conocimientos que el autor del presente trabajo tiene del proceso, debido a lo anterior; la característica primordial para la selección de la metodología será cubrir los objetivos de seguridad como son: confidencialidad, integridad, y disponibilidad.

Con los resultados que arrojaron las tablas de comparación se ha elegido utilizar la metodología Magerit, además se tienen en cuenta las siguientes características:

- Ayuda a descubrir y planificar las medidas oportunas para mantener los riesgos bajo control.
- Es un método sistemático para análisis de riesgos.
- El resultado se expresa en valores económicos.

- Concientización de los dueños del proceso de la existencia de riesgos y la necesidad de controlarlos a tiempo.
- Es un apoyo que permite la preparación para procesos de evaluación, auditoria, certificación o acreditación.
- Cualquier decisión que se tome y tenga que ser validada ante la alta dirección, es fundamentada y evidenciable.

3.3. FASE 2: DESCRIPCIÓN DE LA METODOLOGÍA DE ANÁLISIS Y TRATAMIENTO DE RIESGOS

La metodología Magerit se desarrolla mediante la ejecución de una serie de pasos, los cuales son:

3.3.1. Paso 1: Identificación y valoración de activos.

La metodología Magerit define activo como los "Recursos del sistema de información o relacionados con este, necesarios para que la organización funcione correctamente y alcance los objetivos propuestos por su dirección"[15] y los identifica y divide de la siguiente manera:

Datos / Información: Es el activo esencial de la organización, ósea los datos que se generan y procesan.

Aplicaciones Informáticas: Es el software que permite el manejo de la información o datos.

Equipos informáticos: Es el hardware que permite el almacenamiento de la información o datos, de las aplicaciones y servicios.

Equipamiento Auxiliar: Todos los equipos que son apoyo para los equipos informáticos.

Servicios: Son los activos que se pueden prestar,así como los que son necesarios para el procesamiento o gestión de la información.

Redes de comunicaciones: Son los activos que permiten el intercambio de información o datos.

Instalaciones: Son los activos en donde están alojados los equipos informáticos y de comunicaciones.

[15]MINISTERIO DE ADMINISTRACIONES PÚBLICAS. Metodología de Análisis y gestión de riesgos de los sistemas de información. Madrid, 2006. 17 p

Personal: Personal que administra y manipula todos los activos anteriormente citados.

Para realizar la valoración de activos, Magerit propone dos tipo de valoración; la valoración cualitativa y la valoración cuantitativa.

La valoración cualitativa permite avanzar con rapidez, posicionando el valor de cada activo en un orden relativo respecto a los demás. La limitación de las valoraciones cualitativas es que no permiten comparar valores más allá de su orden relativo. No se pueden sumar valores.

La valoración cuantitativa, es aquella que permite la obtención de la información a partir de la cuantificación de los datos sobre variables[16]. Las dimensiones de seguridad sobre las cuales se realizara la valoración cuantitativa de los activos son:

Confidencialidad (C): es cuando la información no se coloca a disposición ni se revela a individuos, entidades o procesos no autorizados.

Integridad (I): es el mantenimiento de la exactitud y estado completo de la información y sus métodos de proceso.

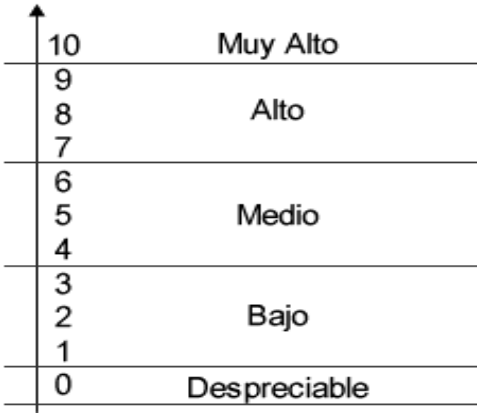
Disponibilidad (D): es el acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran[17].

Magerit utiliza la siguiente escala estándar, va del 0 al 10 siendo el (0) un valor despreciable y (10) el valor más alto.

[16]¿Qué es una metodología? [on line]. [Fecha de consulta: 10 de Diciembre de 2011]. Disponible en http://www.misrespuestas.com/que-es-una-metodologia.html

[17]VALENCIA, Alfonso. Presentación Gestión de la seguridad informática. Bogotá. Universidad Piloto de Colombia, 2010. 44 p.

Figura 4. Escala de valoración de activos



Fuente: Libro II. Catálogo de elementos. Metodología Magerit.

Está escala permite calcular el daño del activo en ausencia de alguna de las dimensiones de seguridad dado que los activos tienen un valor dentro del proceso de mesa de ayuda por los siguientes motivos.

- Seguridad de la información.
- Información de carácter personal.
- Obligaciones jurídicas o legales.
- Intereses económicos.
- Pérdidas Financieras.
- Interrupción del servicio.
- Publicidad o imagen.

Así mismo cada valor dentro de la escala representa un criterio de niveles de daño ocasionado por la ausencia de confidencialidad, disponibilidad e integridad como se ve en la siguiente tabla:

Tabla 4. Tabla de criterios de valoración de activos de mesa de ayuda.

VALOR			CRITERIO
10	Muy Alto	**MA**	Daño Muy grave
7-9	Alto	**A**	Daño Grave
4-6	Medio	**M**	Daño Importante
1-3	Bajo	**B**	Daño Menor
0	Despreciable	**MB**	Irrelevante

Fuente: Libro II. Catálogo de elementos. Metodología Magerit.

Para continuar con la descripción de los elementos que componen la tabla seguiremos explicando cada rango de criterios:

Se puede considerar Daño muy grave [10] a:

- Daños excepcionalmente serios que pueden afectar la eficacia o la seguridad del objetivo operativo o logístico de la mesa de ayuda.
- Daños que pueden causar un incumplimiento grave de una ley, contrato o normas ya sean externas o internas.
- Daños que puedan causar un incidente serio de seguridad y dificulte la investigación de los mismos.
- Daños que pueden causar serias pérdidas económicas.

Daños que pueden causar la pérdida de confidencialidad de Datos o información clasificada como secreta para la mesa de ayuda.Se puede considerar daño Grave [7-9] a:

- Daños que pueden causar una interrupción de las actividades de la mesa de ayuda con un impacto para las demás áreas de la organización.
- Daños que pueden causar una publicidad negativa de la mesa de ayuda a nivel general con las demás áreas de la organización.
- Daños que pueden causar la pérdida de confidencialidad de Datos o información clasificada como reservada o confidencial para la mesa de ayuda.

Se puede considerar daño Importante [4-6] a:

- Daños que pueden afectar labores de un grupo de individuos de la mesa de ayuda.
- Daños que pueden causar la pérdida de confidencialidad de Datos o información clasificada como de difusión limitada para la mesa de ayuda.
- Daños que pueden causar la interrupción de actividades propias de la mesa de ayuda.

Se puede considerar daño menor [1-3] a:

- Daños que probablemente causen interrupción de las actividades propias de la mesa de ayuda.
- Daños que probablemente afecten la eficacia o la seguridad del objetivo operativo o logístico de la mesa de ayuda.
- Daños que probablemente afecten a un individuo de la mesa de ayuda.
- Daños que probablemente causen un incumplimiento de una ley, contrato o normas ya sean externas o internas.
- Daños que pueden causar mal manejo de información clasificada como sin clasificar para la mesa de ayuda.

Se puede considerar daño despreciable [0] a:

- Daños que no afectan las actividades propias de la mesa de ayuda.

- Daños que no afectan la eficacia o la seguridad del objetivo operativo o logístico de la mesa de ayuda.
- Daños que no afectan a los individuos de la mesa de ayuda.

Daño que no causan incumplimiento de una ley, contrato o normas ya sean externas o internas.[18]

La suma de la valoración de las tres variables sobre el activo determina el valor total del activo en el proceso de mesa de ayuda. El valor máximo de un activo es 30 y mínimo es 0. La valoración total del activo será clasificada con la siguiente escala de colores:

Tabla 5. Tabla de clasificación de valoración de activos en escala de colores.

VALOR	CLASIFICACIÓN
0 - 10	Bajo
10- 20	Medio
20 - 30	Alto

Fuente: El autor.

3.3.2. Paso 2: Identificación y valoración de amenazas.

El siguiente paso en la metodología MAGERIT consiste en determinar las amenazas que pueden afectar a cada activo. La metodología MAGERIT identifica y clasifica los siguientes tipos de amenazas de la siguiente manera:

- Desastres Naturales: Sucesos que pueden ocurrir sin intervención de los seres humanos como causa directa o indirecta. en esta categoría se encuentran incendios, inundaciones o demás desastres naturales.

- Desastres de origen industrial: Sucesos que pueden ocurrir de forma accidental, derivados de la actividad humana de tipo industrial; estas amenazas pueden darse de forma accidental o deliberada. En esta categoría se encuentran incendios, daños por agua, desastres industriales, contaminación mecánica, contaminación electromagnética, averia de origen físico o lógico, corte del suministro eléctrico, condiciones inadecuadas de temperatura y/o humedad, fallo de servicios o comunicaciones, interrupción de otros servicios y suministros esenciales, degradación de los soportes de almacenamiento de la información y emanaciones electromagnéticas.

- Errores y Fallos no intencionados: Fallos no intencionales causados por las personas. En esta categoría se encuentran errores de los usuarios, errores

[18]MINISTERIO DE ADMINISTRACIONES PÚBLICAS. Metodología de Análisis y gestión de riesgos de los sistemas de información – Libro II. Catalogo de elementos. Madrid, 2006. 20 p

del administrador, errores de monitorización, errores de configuración, deficiencias de la organización, difusión de software dañino, errores de re-encaminamiento, errores de secuencia, escapes de información, alteración de la información, introducción de información incorrecta, degradación de la información, destrucción de información, divulgación de información, vulnerabilidades de los programas, errores de mantenimiento / actualización de programas, errores de mantenimiento, actualización de equipos, caída del sistema por agotamiento de recurso e indisponibilidad del personal.

- Ataques intencionados: Fallos deliberados causados por las personas. En esta categoría se encuentran Manipulación de la configuración, suplantación de la identidad del usuario, abuso de privilegios de acceso, uso no previsto, difusión de software dañino, re-encaminamiento de mensajes, alteración de secuencia, acceso no autorizado, análisis de tráfico, repudio, interceptación de información, modificación de la información, introducción de falsa información, corrupción de la información, destrucción de la información, divulgación de la información, manipulación de programas, denegación de servicios, robo, ataque destructivo, ocupación enemiga, indisponibilidad del personal, extorsión e ingeniería social.[19]

Una amenaza no afecta a un activo totalmente sino que lo puede afectar en alguna de sus dimensiones de seguridad y en alguna magnitud determinada.

Cuando se ha determinado si una amenaza afecta un activo se debe estimar cuan vulnerable es el activo en dos sentidos.

Degradación o Impacto: Que tan perjudicado resultaría el activo.

Frecuencia: Cada cuanto se materializa la amenaza.

Para realizar una medición de estos dos valores sobre los activos, la metodología Magerit determina la siguiente tabla de valoración.

[19]MINISTERIO DE ADMINISTRACIONES PÚBLICAS. Metodología de Análisis y gestión de riesgos de los sistemas de información – Libro II. Catalogo de elementos. Madrid, 2006. 27 p

Tabla 6. Tabla de valoración de frecuencia y degradación o impacto.

FRECUENCIA (Tasa anual de ocurrencia)	**DESCRIPCION**	**DEGRADACIÓN o IMPACTO**	**DESCRIPCION**
5	Muy frecuente (A diario)	5	Muy Alta(o)
4	Frecuente (Mensual)	4	Alta(o)
3	Normal (Una vez al año)	3	Media(o)
2	Poco Frecuente (Cada varios años)	2	Baja(o)
1	Nunca ocurre	1	Sin degradación o Impacto

Fuente: El autor

3.3.3. Paso 3: Determinación del riesgo.

El riesgo, es la medida del daño probable sobre un sistema. Al conocer el impacto de las amenazas sobre los activos, se puede determinar el riesgo teniendo en cuenta la frecuencia de la ocurrencia. El riesgo crece con el impacto y con la frecuencia.

La siguiente fórmula matemática permite determinar el valor del riesgo que tiene un activo de información.

Vr. Total de Activo.	**X**	**Vr. Frecuencia de Amenaza.**	**X**	**Vr. Degradación o Impacto.**	**=**	**Vr. Riesgo.**

Conociendo el valor total del riesgo y el nivel que representa; en la siguiente tabla se define a que riesgos se les debe hacer un proceso de tratamiento de riesgos.

Tabla 7. Tabla Escala de valoración de Riesgos.

VR. RIESGO	NIVEL		TRATAMIENTO
0 – 149	Bajo	Aceptable	Aceptar el riesgo, se debe realizar un análisis del costo beneficio con el que se pueda decidir entre asumir el riesgo o compartirlo.
150 – 299	Medio	Importante	Reducir, Compartir o transferir el riesgo. La organización debe diseñar planes de contingencia, para protegerse en caso de que se materialicen riesgos de este nivel.
300 - 750	Alto	Inaceptable	Evitar, Reducir, Compartir o transferir el riesgo. Es aconsejable eliminar la actividad que genera el riesgo en la medida que sea posible, de lo contrario se deben implementar controles de prevención para evitar la Probabilidad del riesgo, de Protección para disminuir el Impacto o compartir o transferir el riesgo si es posible a través de pólizas de seguros u otras opciones que estén disponibles

Fuente: El autor

3.3.4. Paso 4: Identificación y valoración de salvaguardas.

Las salvaguardas son aquellas medidas, procedimientos o mecanismos tecnológicos que reducen el riesgo en un proceso o activo. Es necesario identificar las salvaguardas existentes para valorar si están protegiendo a los activos de las amenazas de una manera adecuada y aceptable.

Las salvaguardas también entran en el cálculo del riesgo de dos formas: Cuando reducen la frecuencia de las amenazas son las llamadas salvaguardas preventivas. Las salvaguardas preventivas ideales llegan a impedir completamente que laamenaza se materialice.

Las que limitan el daño causado son las salvaguardas que directamente limitan la posible degradación, mientras que otras permitendetectar inmediatamente el ataque para frenar que la degradación avance. Incluso algunassalvaguardas se limitan a permitir la pronta recuperación del sistema cuando la amenazalo destruye. En cualquiera de las versiones, la amenaza se materializa; pero las consecuencias se limitan.

Las salvaguardas se caracterizan por su existencia y por su eficacia frente al riesgoque pretenden conjurar. La salvaguarda ideal es 100% eficaz, lo que implica que:

• Es teóricamente idónea.
• Está perfectamente desplegada, configurada y mantenida.

• Se emplea siempre.
• 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 están de adorno y el 100% para aquellas que sonperfectas, se estimará un grado de eficacia real en cada caso concreto.

Hay diferentes aspectos en los cuales puede actuar una salvaguarda para alcanzar sus objetivos de limitación del impacto y/o mitigación del riesgo:

Procedimientos: Siempre son necesarios, a veces bastan procedimientos, pero otrasveces los procedimientos son un componente de una salvaguarda más compleja. Se requierenprocedimientos tanto para la operación de las salvaguardas preventivas como para lagestión de incidencias y la recuperación tras las mismas. Los procedimientos deben cubriraspectos tan diversos como van del desarrollo de sistemas la configuración del equipamiento.

Políticas de personal: Son necesarias cuando se consideran sistemas atendidos porpersonal. La política de personal debe cubrir desde las fases de especificación del puesto detrabajo y selección, hasta la formación continua.

Soluciones técnicas: Frecuentes en el entorno de las tecnologías de la información, que puedenser soluciones técnicas para aplicaciones, soluciones técnicas para dispositivos físicos, soluciones técnicas para protección de las comunicaciones y soluciones técnicas para seguridad físicade los locales y áreas de trabajo.

La protección integral de un sistema de información requerirá una combinación de salvaguardasde los diferentes aspectos comentados, caracterizando la solución final que permita estar equilibrada en los diferentes aspectos, que tenga en cuenta las salvaguardas adecuadas a cada tipo de activos, que tenga en cuenta las salvaguardas adecuadas a la dimensión de valor del activo y que tenga en cuenta las salvaguardas adecuadas a la amenaza a minimizar.

Las salvaguardas técnicasvarían con el avance tecnológico ya que aparecen tecnologías nuevas y desaparecen tecnologías antiguas; porque cambian los [tipos de] activos a considerar; porque evolucionan las posibilidades de los atacantes o porque evoluciona el catálogo de salvaguardas disponibles.[20]

[20]MINISTERIO DE ADMINISTRACIONES PÚBLICAS. Metodología de Análisis y gestión de riesgos de los sistemas de información – Libro II. Catálogo de elementos. Madrid, 2006. 48 p

La metodología Magerit da una valoración a las salvaguardas de la siguiente manera:

La valoración de la efectividad se ha realizado sobre una escala de 4 valores.

Tabla 8. Tabla de valoración de Salvaguardas

EFECTIVIDAD	DESCRIPCION
100% - 75%	Efectividad muy alta: Salvaguarda diseñada específicamente para la amenaza.
74% - 50%	Efectividad alta: Reduce la frecuencia o la degradación de la amenaza sobre el activo significativamente.
49% - 25%	Efectividad Media: La salvaguarda tiene un impacto indirecto o general sobre la amenaza.
24% - 0%	Efectividad Baja: Tiene un impacto muy bajo sobre la amenaza o en el peor de los casos (0) no tiene ningún impacto sobre dicha amenaza.

Fuente: Libro II. Catálogo de elementos. Metodología Magerit.

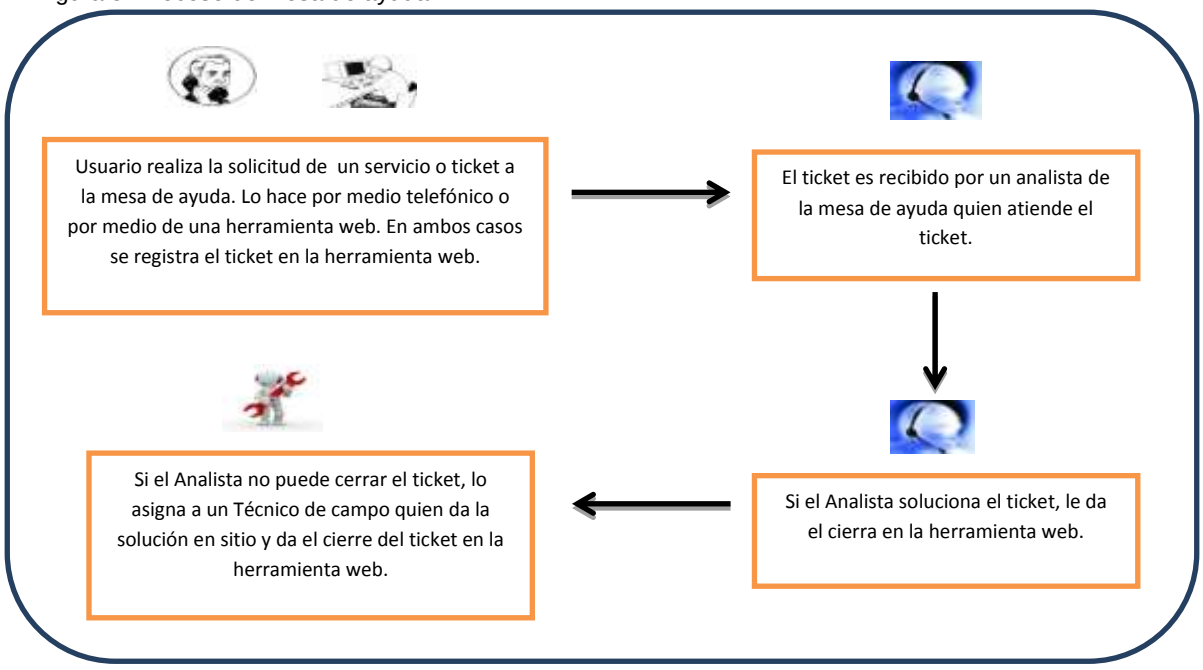
3.4. FASE 3:DESARROLLO DE LA METODOLOGÍA DE ANÁLISIS Y TRATAMIENTO DE RIESGOS.

3.4.1. Identificación de Activos de la mesa de ayuda.

Teniendo en cuenta la anterior identificación de activos que ofrece la metodología Magerit, en la siguiente tabla se identificaran y clasificaran los activos de información por tipo que hacen parte de una mesa de ayuda con su respectiva descripción; Se hace referencia nuevamente a la delimitación de la mesa de ayuda que se ha dado en este trabajo para el levantamiento de activos de información.“Mesa de ayuda integrada por analistas los cuales atienden solicitudes de problemas tecnológicos de una organización financiera como lo es un banco, estas solicitudes conocidas como tickets o servicios se reciben por medio de una herramienta web o por medio de llamada telefónica. La mesa de ayuda puede ser un área directa de la organización o un área que hace parte de un outsourcing que presta el servicio.”

Para entender mejor el proceso básico que se cumple en una mesa de ayuda tecnológica y así poder identificar los activos de información; se muestra el siguiente gráfico que muestra el proceso de la mesa de ayuda.

Figura 5. Proceso de Mesa de ayuda.



Fuente: El autor.

Tabla 9. Tabla de identificación de activos de mesa de ayuda.

TIPO DE ACTIVO	NOMBRE DEL ACTIVO	DESCRIPCION
DATOS / INFORMACIÓN (D/I)	Base de datos de tickets	Base de datos en donde se registra la información correspondiente a los tickets abiertos por los usuarios.
	Manuales de aplicaciones	Manuales de configuración y solución de inconvenientes de aplicaciones.
	Manuales de procedimientos operacionales	Manuales de procedimientos operacionales.
APLICACIONES INFORMÁTICAS (SW)	Correo Electrónico	Permite la comunicación con los usuarios internos y externos.
	Aplicación Web para manejo de Tickets	Aplicación que permite administrar los tickets que son abiertos por los usuarios.
	Aplicación para conexión remota	Aplicación que permite la conexión remota entre estaciones de trabajo para dar atención a los tickets
EQUIPOS INFORMÁTICOS (HW)	Computadores	Estaciones de trabajo de los analistas de la mesa de ayuda.
	Teléfonos	Permiten la comunicación con los usuarios internos y externos.
	Servidor Base de Datos y Herramienta Web	Servidor de Base de datos y de la herramienta web
EQUIPAMIENTO AUXILIAR (AUX)	Servicio de red	Soporta todas la interacciones de conectividad entre la mesa de ayuda y los usuarios
	Servicio Eléctrico	Base para el funcionamiento de la plataforma tecnológica y de las estaciones de trabajo de los analistas de la mesa de ayuda.
	Servicio de telefonía	Servicio que permite la comunicación telefónica con los usuarios.
SERVICIOS (S)	Soporte	Soporte a usuarios dando solución a errores de software, hardware y perfiles.
REDES DE COMUNICACIONES (COM)	Internet	Permite que funcione la herramienta web.
PERSONAL (P)	Analistas Mesa de ayuda	Personas encargadas de dar soporte en la mesa de ayuda a los usuarios.

Fuente: El autor.

3.4.2. Valoración de activos de mesa de ayuda.

Al realizar la valoración de activos de la mesa de ayuda, la tabla desarrollada permite ver el valor que tienen los activos en cada una de las variables de seguridad; la tabla de valoración que surge es la siguiente teniendo en cuenta las siguientes características de los activos.

- **Base de datos de tickets:** Permite que se tenga un histórico de los tickets que se han realizado, su confidencialidad debe ser alta, no interfiere en el proceso si no está disponible o integra por un tiempo medio.

- **Manuales de aplicaciones y procedimientos operacionales:** Son consultados por los analistas para el conocimiento y aplicación de los procedimientos operacionales de la mesa de ayuda y la instalación y reparación de las aplicaciones de la organización; su confidencialidad debe ser alta, si no están disponibles o íntegros afectan de una manera significativa el objetivo de soporte de la mesa de ayuda.

- **Correo Electrónico:** Permite la comunicación entre los analistas de la mesa de ayuda y los empleados de la organización, su confidencialidad debe ser media, su integridad y disponibilidad no interfieren en el proceso.

- **Aplicación Web para manejo de Tickets:** Herramienta que permite la apertura y administración de tickets por los empleados y por los analistas; no requiere de una confidencialidad alta, y su integridad y disponibilidad si debe ser media ya que se tiene como opción alterna la recepción de tickets por medio telefónico.

- **Aplicación para conexión remota:** Herramienta que permite la conexión remota para dar solución a los tickets; su confidencialidad, integridad y disponibilidad puede ser mínima ya que no interfiere en el proceso ya que si no está disponible, el ticket lo puede manejar el técnico de soporte en sitio.

- **Computadores:** Usados por los analistas para el cumplimiento de sus funciones; su confidencialidad debe ser media, su integridad y disponibilidad si debe ser alta para la atención de los tickets y cumplimiento del objetivo de la mesa de ayuda.

- **Teléfonos:**Usados por los analistas para la atención de las llamadas de los empleados de la organización; su confidencialidad, integridad y disponibilidad debe ser alta.

- **Servidor Base de Datos y Herramienta Web:** Servidor en el que se aloja la plataforma de base de datos y de la herramienta web; su confidencialidad, integridad y disponibilidad debe ser alta.

- **Servicio de red:** Soporta todas la interacciones de conectividad entre la mesa de ayuda y los usuarios; su confidencialidad debe ser alta, su integridad y disponibilidad debe ser media ya que se tiene como opción alterna la atención de tickets por medio telefónico.

- **Servicio Eléctrico:** Base para el funcionamiento de la plataforma tecnológica y de las estaciones de trabajo de los analistas de la mesa de ayuda; su confidencialidad no se valora por sus características como tipo de activo, pero su integridad y disponibilidad si debe ser alta porque es la base del funcionamiento de los elementos tecnológicos de la mesa de ayuda.

- **Servicio de Telefonia:** Servicio que permite la comunicación telefónica con los empleados de la organización; su confidencialidad debe ser alta, su integridad y disponibilidad debe ser media.

- **Soporte:** Soporte a usuarios dando solución a errores de software, hardware y perfiles; su confidencialidad no se valora por sus características como tipo de activo, su integridad y disponibilidad debe ser alta para el cumplimiento del objetivo de la mesa de ayuda.

- **Internet:** Permite que funcione la herramienta web; su confidencialidad, integridad y disponibilidad puede ser media ya que también se utiliza el servicio de telefonía.

- **Analistas mesa de ayuda:** Personas encargadas de dar soporte en la mesa de ayuda a los usuarios; por sus características como tipo de activo su confidencialidad no se valora, su integridad y disponibilidad si debe ser alta.

Tabla 10. Tabla de valoración de activos de mesa de ayuda.

TIPO DE ACTIVO	NOMBRE DEL ACTIVO	VALORACIÓN			VALORACIÓN TOTAL DEL ACTIVO (C+I+D)
		C	I	D	
DATOS / INFORMACIÓN (D/I)	Base de datos de tickets	9	6	5	20
	Manuales de aplicaciones	9	8	4	21
	Manuales de procedimientos operacionales	9	8	4	21
APLICACIONES INFORMÁTICAS (SW)	Correo Electrónico	7	3	3	13
	Aplicación Web para manejo de Tickets	4	7	7	18
	Aplicación para conexión remota	3	3	3	9
EQUIPOS INFORMÁTICOS (HW)	Computadores	6	9	9	24
	Teléfonos	8	8	8	24
	Servidor Base de Datos y Herramienta Web	9	9	9	27
EQUIPAMIENTO AUXILIAR (AUX)	Servicio de red	9	6	6	21
	Servicio Eléctrico	0	9	9	18
	Servicio de telefonía	9	6	6	21
SERVICIOS (S)	Soporte	0	9	9	18
REDES DE COMUNICACIONES (COM)	Internet	6	5	5	16
PERSONAL (P)	Analistas Mesa de ayuda	0	10	10	20

Fuente: El autor.

3.4.3. Identificación y valoración de amenazas.

En el siguiente cuadro se identifican y valoran las amenazas más importantes a las que están expuestos los activos de la mesa de ayuda.

Las amenazas identificadas corresponden al listado que suministra la metodología Magerit en su Libro II. Catalogo de elementos.

Según el tipo de activo se identificaron las amenazas más importantes así:

Acceso no autorizado: Amenaza en la que el atacante consigue acceder a los recursos del sistema sin tener autorización para ello, típicamenteaprovechando un fallo del sistema de identificación y autorización.

Alteración de la Información: Alteración accidental de la información, esta amenaza sólo se identifica sobre datos en general, pues cuando la información está enalgún soporte informático, hay amenazas específicas.

Análisis de tráfico: Amenaza en la que el atacante, sin necesidad de entrar a analizar el contenido de las comunicaciones, es capazde extraer conclusiones a partir del análisis del origen, destino, volumen y frecuencia de los intercambios. A veces se denomina “monitorización de tráfico”.

Avería de origen físico o lógico:Fallos en los equipos y/o fallos en los programas. Puede ser debida a un defecto de origen osobrevenida durante el funcionamiento del sistema.En sistemas de propósito específico, a veces es difícil saber si el origen del fallo es físico o lógico; pero para las consecuencias que se derivan, esta distinción no suele ser relevante.

Contaminación electromagnética: Amenaza relacionada con interferencias de radio, campos magnéticos, luz ultravioleta.

Corte del suministro eléctrico:Amenaza que se refiere al cese de la alimentación de potencia.

Daños por agua: Escapes, fugas, inundaciones: posibilidad de que el agua acabe con los recursos del sistema.

Deficiencias en la organización: Cuando no está claro quién tiene que hacer exactamente qué y cuándo, incluyendo tomar medidassobre los activos o informar a la jerarquía de gestión.Acciones descoordinadas, errores por omisión, etc.

Denegación de servicio: Amenaza que existe por la carencia de recursos suficientes que provoca la caída del sistema cuando la carga de trabajo esdesmesurada.

Destrucción de la información: Pérdida accidental de información.Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está enalgún soporte informático, hay amenazas específicas.

Difusión de software dañino: Propagación inocente de virus, espías (spyware), gusanos, troyanos, bombas lógicas, etc.

Errores de configuración: Amenaza que existe por la introducción de datos de configuración erróneos.Prácticamente todos los activos dependen de su configuración y ésta de la diligencia del administrador:privilegios de acceso, flujos de actividades, registro de actividad, encaminamiento,etc.

Errores de los usuarios:Amenaza que existe por las equivocaciones de las personas cuando usan los servicios, datos, etc.

Errores de mantenimiento / actualización de equipos: Defectos en los procedimientos o controles de actualización de los equipos que permiten quesigan utilizándose más allá del tiempo nominal de uso.

Errores de mantenimiento / actualización de programas: Defectos en los procedimientos o controles de actualización del código que permiten que sigan utilizándose programas con defectos conocidos y reparados por el fabricante.

Errores del administrador: Amenaza que existe por equivocaciones de personas con responsabilidades de instalación y operación.

Extorsión: Presión que, mediante amenazas, se ejerce sobre alguien para obligarle a obrar en determinadosentido.

Fallo de Servicios de comunicaciones: Amenaza que se da por el cese de la capacidad de transmitir datos de un sitio a otro. Típicamente se debe a la destrucciónfísica de los medios físicos de transporte o a la detención de los centros de conmutación,sea por destrucción, detención o simple incapacidad para atender al tráfico presente.

Indisponibilidad del personal: Amenaza por la ausencia accidental del puesto de trabajo: enfermedad, alteraciones del orden público, guerrabacteriológica y ausencia deliberada del puesto de trabajo: como huelgas, absentismo laboral, bajas no justificadas, bloqueo de los accesos.

Ingeniería social: Abuso de la buena fe de las personas para que realicen actividades que interesan a un tercero.

Repudio: Negación a posteriori de actuaciones o compromisos adquiridos en el pasado.Repudio de origen: negación de ser el remitente u origen de un mensaje o comunicación.Repudio de recepción: negación de haber recibido un mensaje o comunicación.Repudio de entrega: negación de haber recibido un mensaje para su entrega a otro.

Robo: La sustracción de equipamiento provoca directamente la carencia de un medio para prestar losservicios, es decir una indisponibilidad.El robo puede afectar a todo tipo de equipamiento, siendo el robo de equipos y el robo de soportesde información los más habituales.El robo puede realizarlo personal interno, personas ajenas a la Organización o personas contratadasde forma temporal, lo que establece diferentes grados de facilidad para acceder alobjeto sustraído y diferentes consecuencias.En el caso de equipos que hospedan datos, además se puede sufrir una fuga de información.

Uso no previsto: Utilización de los recursos del sistema para fines no previstos, típicamente de interés personal:juegos, consultas personales en Internet, bases de datos personales, programas personales,almacenamiento de datos personales, etc.

Vulnerabilidades de los programas: Defectos en el código que dan pie a una operación defectuosa sin intención por parte delusuario pero con consecuencias sobre la integridad de los datos o la capacidad misma deoperar.

Tabla 11. Tabla de identificación y valoración de amenazas.

TIPO DE ACTIVO	NOMBRE DEL ACTIVO	AMENAZAS	FRECUENCIA	DEGRADACION o IMPACTO
DATOS / INFORMACIÓN (D/I)	Base de datos de tickets / Manuales de aplicaciones / Manuales de procedimientos operacionales	Errores del administrador	3	4
		Acceso no autorizado	2	5
		Robo / Robo de información	1	5
		Alteración de la información	2	5
		Destrucción de la información	1	5
APLICACIONES INFORMÁTICAS (SW)	Correo Electrónico / Aplicación Web para manejo de Tickets / Aplicación para conexión remota	Avería de origen físico o lógico	3	3
		Errores de configuración	3	4
		Difusión de software dañino	2	4
		Vulnerabilidades de los programas	2	5
		Errores de mantenimiento / actualización de programas	2	5
		Acceso no autorizado	2	4
EQUIPOS INFORMÁTICOS (HW)	Computadores / Teléfonos / Servidor de Base de Datos y Herramienta Web	Daños por agua	2	5
		Avería de origen físico o lógico	3	5

Continuación EQUIPOS INFORMÁTICOS (HW)	Continuación Computadores / Teléfonos / Servidor de Base de Datos y Herramienta Web	Corte del suministro eléctrico	2	5
		Errores de configuración	3	4
		Errores de mantenimiento / actualización de equipos	2	5
		Uso no previsto	4	2
		Robo / Robo de información	1	5
		Acceso no autorizado	2	4
EQUIPAMIENTO AUXILIAR (AUX)	Servicio de red / Servicio Eléctrico / Servicio de telefonía	Contaminación electromagnética	2	2
		Avería de origen físico o lógico	3	5
		Corte del suministro eléctrico	2	5
		Fallo de servicios de comunicaciones	2	5
		Denegación de servicio	2	4
SERVICIOS (S)	Soporte	Errores de los usuarios	3	3
		Repudio	3	5
REDES DE COMUNICACIONES (COM)	Internet	Avería de origen físico o lógico	3	5
		Fallo de servicios de comunicaciones	3	4

continuación REDES DE COMUNICACIONES (COM)	Continuación Internet	Uso no previsto	4	2
		Análisis de tráfico	1	4
PERSONAL (P)	Analistas Mesa de ayuda	Deficiencias en la organización	3	3
		Indisponibilidad del personal	4	3
		Extorsión	1	5
		Ingeniería Social	3	4

Fuente: El autor.

3.4.4. Identificación y valoración del riesgo.

En el siguiente cuadro se identifican y valoran los riesgos más importantes a los que están expuestos los activos de la mesa de ayuda según las amenazas a las que está expuesto.

Las amenazas identificadas corresponden al listado que suministra la metodología Magerit en su Libro II. Catalogo de elementos.

Los riesgos asociados a las amenazas son los riesgos más comunes que se generan por cada una de las mismas; se hace la aclaración ya que por una misma amenaza se pueden generar múltiples riesgos, pero solamente se tratan los más importantes y comunes.

Tabla 12. Tabla de identificación y valoración deriesgos.

TIPO DE ACTIVO	NOMBRE DEL ACTIVO	VR. TOTAL ACTIVO	AMENAZAS	FRECUENCIA	DEGRADACION o IMPACTO	RIESGO ASOCIADO A LA AMENAZA	VALOR RIESGO
DATOS / INFORMACIÓN (D/I)	Base de datos de tickets	20	Errores del administrador	3	4	Perdida de Integridad en la base de datos	240
			Acceso no autorizado	2	5	Perdida de Integridad y confidencialidad en la base de datos	200
			Robo de información	1	5	No disponibilidad de la base de datos	100
			Alteración de la información	2	5	Errores en la operación	200
			Destrucción de la información	1	5	No disponibilidad de la base de datos	100
	Manuales de aplicaciones	21	Errores del administrador	3	4	Perdida de integridad de los manuales	252
			Acceso no autorizado	2	5	Perdida de Integridad y confidencialidad de los manuales	210
			Robo de información	1	5	No disponibilidad de los manuales	105
			Alteración de la información	2	5	Errores en la operación	210
			Destrucción de la información	1	5	No disponibilidad de los manuales	105
	Manuales de	21	Errores del administrador	3	4	Perdida de	252

Continuación DATOS / INFORMACIÓN (D/I)	procedimientos operacionales					integridad de los manuales	
			Acceso no autorizado	2	5	Perdida de Integridad y confidencialidad de los manuales	210
			Robo de información	1	5	No disponibilidad de los manuales	105
			Alteración de la información	2	5	Errores en la operación	210
			Destrucción de la información	1	5	No disponibilidad de los manuales	105
APLICACIONES INFORMÁTICAS (SW)	Correo Electrónico	13	Avería de origen físico o lógico	3	3	No disponibilidad del correo electrónico	117
			Errores de configuración	3	4	No disponibilidad del correo electrónico	156
			Difusión de software dañino	2	4	Daño en el aplicativo de correo electrónico	104
			Vulnerabilidades de los programas	2	5	Daño en el aplicativo de correo electrónico	130
			Errores de mantenimiento / actualización de programas	2	5	No disponibilidad del correo electrónico	130
			Acceso no autorizado	2	4	Perdida de confidencialidad del correo electrónico	104
	Aplicación Web para manejo de Tickets	18	Avería de origen físico o lógico	3	3	No disponibilidad del aplicativo web	162
			Errores de configuración	3	4	Errores en la operación	216

Continuación APLICACIONES INFORMÁTICAS (SW)			Difusión de software dañino	2	4	No disponibilidad del aplicativo web	144
			Vulnerabilidades de los programas	2	5	Daño en el aplicativo web	180
			Errores de mantenimiento / actualización de programas	2	5	No disponibilidad del aplicativo web	180
			Acceso no autorizado	2	4	Uso incorrecto del aplicativo web	144
	Aplicación para conexión remota	9	Avería de origen físico o lógico	3	3	No disponibilidad del aplicativo de conexión remota	81
			Errores de configuración	3	4	Errores en la operación	108
			Difusión de software dañino	2	4	No disponibilidad del aplicativo de conexión remota	72
			Vulnerabilidades de los programas	2	5	Daño en el aplicativo de conexión remota	90
			Errores de mantenimiento / actualización de programas	2	5	No disponibilidad del aplicativo de conexión remota	90
			Acceso no autorizado	2	4	Uso incorrecto del aplicativo de conexión remota	72
EQUIPOS INFORMÁTICOS (HW)	Computadores	24	Daños por agua	2	5	No disponibilidad del computador	240
			Avería de origen físico o lógico	3	5	No disponibilidad del computador	360
			Corte del suministro eléctrico	2	5	No disponibilidad del computador	240
			Errores de configuración	3	4	Errores en la operación	288

Continuación EQUIPOS INFORMÁTICOS (HW)			Errores de mantenimiento / actualización de equipos	2	5	No disponibilidad del computador	240
			Uso no previsto	4	2	Mal uso del recurso asignado	192
			Robo	1	5	No disponibilidad del computador	120
			Acceso no autorizado	2	4	Uso incorrecto del computador	192
	Teléfonos	24	Daños por agua	2	5	No disponibilidad del teléfono	240
			Avería de origen físico o lógico	3	5	No disponibilidad del teléfono	360
			Corte del suministro eléctrico	2	5	No disponibilidad del teléfono	240
			Errores de configuración	3	4	Errores en la operación	288
			Errores de mantenimiento / actualización de equipos	2	5	No disponibilidad del teléfono	240
			Uso no previsto	4	2	Mal uso del recurso asignado	192
			Robo	1	5	No disponibilidad del teléfono	120
			Acceso no autorizado	2	4	Uso incorrecto del teléfono	192
	Servidor de Base de Datos y Herramienta Web	27	Daños por agua	2	5	No disponibilidad del servidor	270
			Avería de origen físico o lógico	3	5	No disponibilidad del servidor	405
			Corte del suministro eléctrico	2	5	No disponibilidad del servidor	270
			Errores de configuración	3	4	Errores en la operación	324

Continuación EQUIPOS INFORMÁTICOS (HW)			Errores de mantenimiento / actualización de equipos	2	5	No disponibilidad del servidor	270
			Uso no previsto	4	2	Mal uso del recurso asignado	216
			Robo	1	5	No disponibilidad del servidor	135
			Acceso no autorizado	2	4	Uso incorrecto del servidor	216
EQUIPAMIENTO AUXILIAR (AUX)	Servicio de red	21	Contaminación electromagnética	2	2	Error en la comunicación de los datos	210
			Avería de origen físico o lógico	3	5	No disponibilidad del servicio	315
			Corte del suministro eléctrico	2	5	No disponibilidad del servicio	210
			Fallo de servicios de comunicaciones	2	5	No disponibilidad del servicio	210
			Denegación de servicio	2	4	No disponibilidad del servicio	168
	Servicio Eléctrico	18	Contaminación electromagnética	2	2	Error en la operación	72
			Avería de origen físico o lógico	3	5	No disponibilidad del servicio	270
			Denegación de servicio	2	4	No disponibilidad del servicio	144
	Servicio de telefonía	21	Contaminación electromagnética	2	2	Error en la comunicación de los datos	84
			Avería de origen físico o lógico	3	5	No disponibilidad del servicio	315
			Corte del suministro eléctrico	2	5	No disponibilidad del servicio	210

Continuación EQUIPAMIENTO AUXILIAR (AUX)			Fallo de servicios de comunicaciones	2	5	No disponibilidad del servicio	210
			Denegación de servicio	2	4	No disponibilidad del servicio	168
SERVICIOS (S)	Soporte	18	Errores de los usuarios	3	3	Perdida de reputación	162
			Repudio	3	5	Pérdida de confianza	270
REDES DE COMUNICACIONES (COM)	Internet	16	Avería de origen físico o lógico	3	5	No disponibilidad del servicio	240
			Fallo de servicios de comunicaciones	3	4	No disponibilidad del servicio	192
			Uso no previsto	4	2	Mal uso del recurso asignado	128
			Análisis de tráfico	1	4	Perdida de confidencialidad	64
PERSONAL (P)	Analistas Mesa de ayuda	20	Deficiencias en la organización	3	3	Abandono del trabajo	180
			Indisponibilidad del personal	4	3	Retrasos de atención de la operación	240
			Extorsión	1	5	Perdida de confidencialidad de la operación	100
			Ingeniería Social	3	4	Perdida de confidencialidad de la operación	240

Fuente: El autor.

3.4.5. Identificación y valoración de salvaguardas.

En el siguiente cuadro se identifican y valoran las salvaguardas que nos permiten mitigar las amenazas a las que están expuestos los activos de la mesa de ayuda.

Las amenazas identificadas corresponden al listado que suministra la metodología Magerit en su Libro II. Catalogo de elementos.

Las salvaguardas que se describen en la tabla son las salvaguardas o controles que si se aplican permiten reducir el riesgo a un nivel de riesgo residual el cual también se determina en la tabla.

Tabla 13. Tabla de identificación y valoración de salvaguardas y riesgo residual.

TIPO DE ACTIVO	NOMBRE DEL ACTIVO	VR. TOTAL ACTIVO	AMENAZAS	FRECUENCIA	DEGRADACION o IMPACTO	RIESGO ASOCIADO A LA AMENAZA	VALOR RIESGO	SALVAGUARDA	VALOR SALVAGUARDA %	VR. RIESGO RESIDUAL
DATOS / INFORMACIÓN (D/I)	Base de datos de tickets	20	Errores del administrador	3	4	Perdida de Integridad en la base de datos	240	Pruebas de cambios en el sistema antes de salir a operación	60	96
			Acceso no autorizado	2	5	Perdida de Integridad y confidencialidad en la base de datos	200	Establecimiento de perfiles de usuario	60	80
			Robo de información	1	5	No disponibilidad de la base de datos	100	Aseguramiento de la base de datos	40	60
			Alteración de la información	2	5	Errores en la operación	200	Capacitación al personal	60	80
			Destrucción de la información	1	5	No disponibilidad de la base de datos	100	Copia de respaldo periódica	80	20
	Manuales de aplicaciones	21	Errores del administrador	3	4	Perdida de integridad de los manuales	252	Pruebas de cambios en el sistema antes de salir a operación	60	100,8
			Acceso no autorizado	2	5	Perdida de Integridad y confidencialidad de los manuales	210	Establecimiento de perfiles de usuario	60	84
			Robo de información	1	5	No disponibilidad de los manuales	105	Aseguramiento del medio en donde se encuentran los manuales	40	63
			Alteración de la información	2	5	Errores en la operación	210	Capacitación al personal	60	84
			Destrucción de la información	1	5	No disponibilidad de los manuales	105	Copia de respaldo periódica	80	21

Continuación DATOS / INFORMACIÓN (D/I)	Manuales de procedimientos operacionales	21	Errores del administrador	3	4	Perdida de integridad de los manuales	252	Pruebas de cambios en el sistema antes de salir a operación	60	100,8
			Acceso no autorizado	2	5	Perdida de Integridad y confidencialidad de los manuales	210	Establecimiento de perfiles de usuario	60	84
			Robo de información	1	5	No disponibilidad de los manuales	105	Aseguramiento del medio en donde se encuentran los manuales	40	63
			Alteración de la información	2	5	Errores en la operación	210	Capacitación al personal	60	84
			Destrucción de la información	1	5	No disponibilidad de los manuales	105	Copia de respaldo periodica	80	21
APLICACIONES INFORMÁTICAS (SW)	Correo Electrónico	13	Avería de origen físico o lógico	3	3	No disponibilidad del correo electrónico	117	Soporte por parte del proveedor	40	70,2
			Errores de configuración	3	4	No disponibilidad del correo electrónico	156	Soporte por parte del proveedor	40	93,6
			Difusión de software dañino	2	4	Daño en el aplicativo de correo electrónico	104	Implementación de antivirus	80	20,8
			Vulnerabilidades de los programas	2	5	Daño en el aplicativo de correo electrónico	130	Soporte por parte del proveedor	40	78
			Errores de mantenimiento / actualización de programas	2	5	No disponibilidad del correo electrónico	130	Soporte por parte del proveedor	40	78
			Acceso no autorizado	2	4	Perdida de confidencialidad del correo electrónico	104	Establecimiento de perfiles de usuario	50	52
	Aplicación Web para manejo de Tickets	18	Avería de origen físico o lógico	3	3	No disponibilidad del aplicativo web	162	Soporte por parte del proveedor	40	97,2
			Errores de configuración	3	4	Errores en la operación	216	Soporte por parte del proveedor	40	129,6

Continuación APLICACIONES INFORMÁTICAS (SW)			Difusión de software dañino	2	4	No disponibilidad del aplicativo web	144	Implementación de antivirus	80	28,8
			Vulnerabilidades de los programas	2	5	Daño en el aplicativo web	180	Soporte por parte del proveedor	40	108
			Errores de mantenimiento / actualización de programas	2	5	No disponibilidad del aplicativo web	180	Soporte por parte del proveedor	40	108
			Acceso no autorizado	2	4	Uso incorrecto del aplicativo web	144	Establecimiento de perfiles de usuario	50	72
	Aplicación para conexión remota	9	Avería de origen físico o lógico	3	3	No disponibilidad del aplicativo de conexión remota	81	Soporte por parte del proveedor	40	48,6
			Errores de configuración	3	4	Errores en la operación	108	Soporte por parte del proveedor	40	64,8
			Difusión de software dañino	2	4	No disponibilidad del aplicativo de conexión remota	72	Implementación de antivirus	80	14,4
			Vulnerabilidades de los programas	2	5	Daño en el aplicativo de conexión remota	90	Soporte por parte del proveedor	40	54
			Errores de mantenimiento / actualización de programas	2	5	No disponibilidad del aplicativo de conexión remota	90	Soporte por parte del proveedor	40	54
			Acceso no autorizado	2	4	Uso incorrecto del aplicativo de conexión remota	72	Establecimiento de perfiles de usuario	50	36
EQUIPOS INFORMÁTICOS (HW)	Computadores	24	Daños por agua	2	5	No disponibilidad del computador	240	Establecimiento de políticas de buen uso de recursos	50	120
			Avería de origen físico o lógico	3	5	No disponibilidad del computador	360	Soporte por parte del proveedor	70	108
			Corte del suministro eléctrico	2	5	No disponibilidad del computador	240	Implementación del Sistema de contingencia	70	72

Continuación EQUIPOS INFORMÁTICOS (HW)			Errores de configuración	3	4	Errores en la operación	288	Soporte por parte del proveedor	60	115,2
			Errores de mantenimiento / actualización de equipos	2	5	No disponibilidad del computador	240	Soporte por parte del proveedor	60	96
			Uso no previsto	4	2	Mal uso del recurso asignado	192	Capacitación al personal	60	76,8
			Robo	1	5	No disponibilidad del computador	120	Sistemas y mecanismos de monitoreo y vigilancia	75	30
			Acceso no autorizado	2	4	Uso incorrecto del computador	192	Establecimiento de perfiles de usuario	70	57,6
	Teléfonos	24	Daños por agua	2	5	No disponibilidad del teléfono	240	Establecimiento de políticas de buen uso de recursos	50	120
			Avería de origen físico o lógico	3	5	No disponibilidad del teléfono	360	Soporte por parte del proveedor	70	108
			Corte del suministro eléctrico	2	5	No disponibilidad del teléfono	240	Implementación del Sistema de contingencia	70	72
			Errores de configuración	3	4	Errores en la operación	288	Soporte por parte del proveedor	60	115,2
			Errores de mantenimiento / actualización de equipos	2	5	No disponibilidad del teléfono	240	Soporte por parte del proveedor	60	96
			Uso no previsto	4	2	Mal uso del recurso asignado	192	Capacitación al personal	60	76,8
			Robo	1	5	No disponibilidad del teléfono	120	Sistemas y mecanismos de monitoreo y vigilancia	75	30
			Acceso no autorizado	2	4	Uso incorrecto del teléfono	192	Establecimiento de perfiles de usuario	70	57,6

Continuación EQUIPOS INFORMÁTICOS (HW)	Servidor de Base de Datos y Herramienta Web	27	Daños por agua	2	5	No disponibilidad del servidor	270	Centro de computo acondicionado a la normatividad	50	135
			Avería de origen físico o lógico	3	5	No disponibilidad del servidor	405	Soporte por parte del proveedor	70	121,5
			Corte del suministro eléctrico	2	5	No disponibilidad del servidor	270	Implementación del Sistema de contingencia	70	81
			Errores de configuración	3	4	Errores en la operación	324	Soporte por parte del proveedor	60	129,6
			Errores de mantenimiento / actualización de equipos	2	5	No disponibilidad del servidor	270	Soporte por parte del proveedor	60	108
			Uso no previsto	4	2	Mal uso del recurso asignado	216	Capacitación al personal	60	86,4
			Robo	1	5	No disponibilidad del servidor	135	Sistemas y mecanismos de monitoreo y vigilancia	75	33,75
			Acceso no autorizado	2	4	Uso incorrecto del servidor	216	Establecimiento de perfiles de usuario	70	64,8
EQUIPAMIENTO AUXILIAR (AUX)	Servicio de red	21	Contaminación electromagnética	2	2	Error en la comunicación de los datos	210	Optima Calidad en los elementos que componen la red	80	42
			Avería de origen físico o lógico	3	5	No disponibilidad del servicio	315	Soporte por parte del proveedor	70	94,5
			Corte del suministro eléctrico	2	5	No disponibilidad del servicio	210	Implementación del Sistema de contingencia	70	63
			Fallo de servicios de comunicaciones	2	5	No disponibilidad del servicio	210	Implementación del Sistema de contingencia	70	63
			Denegación de servicio	2	4	No disponibilidad del servicio	168	Implementación del Sistema de contingencia	75	42

Continuación EQUIPAMIENTO AUXILIAR (AUX)	Servicio Eléctrico	18	Contaminación electromagnética	2	2	Error en la operación	72	Optima Calidad en los elementos que componen la red	80	14,4
			Avería de origen físico o lógico	3	5	No disponibilidad del servicio	270	Soporte por parte del proveedor	70	81
			Denegación de servicio	2	4	No disponibilidad del servicio	144	Implementación del Sistema de contingencia	75	36
	Servicio de telefonía	21	Contaminación electromagnética	2	2	Error en la comunicación de los datos	84	Optima Calidad en los elementos que componen la red	80	16,8
			Avería de origen físico o lógico	3	5	No disponibilidad del servicio	315	Soporte por parte del proveedor	70	94,5
			Corte del suministro eléctrico	2	5	No disponibilidad del servicio	210	Implementación del Sistema de contingencia	70	63
			Fallo de servicios de comunicaciones	2	5	No disponibilidad del servicio	210	Implementación del Sistema de contingencia	70	63
			Denegación de servicio	2	4	No disponibilidad del servicio	168	Implementación del Sistema de contingencia	75	42
SERVICIOS (S)	Soporte	18	Errores de los usuarios	3	3	Perdida de reputación	162	Capacitación al personal	75	40,5
			Repudio	3	5	Pérdida de confianza	270	Capacitación al personal	75	67,5
REDES DE COMUNICACIONES (COM)	Internet	16	Avería de origen físico o lógico	3	5	No disponibilidad del servicio	240	Soporte por parte del proveedor	70	72
			Fallo de servicios de comunicaciones	3	4	No disponibilidad del servicio	192	Implementación del Sistema de contingencia	70	57,6
			Uso no previsto	4	2	Mal uso del recurso asignado	128	Capacitación al personal	75	32
			Análisis de tráfico	1	4	Perdida de confidencialidad	64	Sistemas y mecanismos de monitoreo y vigilancia	75	16

PERSONAL (P)	Analistas Mesa de ayuda	20	Deficiencias en la organización	3	3	Abandono del trabajo	180	Revisión de políticas Internas	60	72
			Indisponibilidad del personal	4	3	Retrasos de atención de la operación	240	Medición del capacity	70	72
			Extorsión	1	5	Perdida de confidencialidad de la operación	100	Estudio de Seguridad	50	50
			Ingeniería Social	3	4	Perdida de confidencialidad de la operación	240	Capacitación al personal	70	72

Fuente: El autor.

CONCLUSIONES

- ✓ El presente trabajo corrobora la propuesta planteada donde se quería llegar a plantear una base para la implementación de nuevas mesas de ayuda y la revisión de las que ya están en funcionamiento. Una mesa de ayuda que se crea con lo mínimo que se ha establecido en este trabajo iniciara con una base fuerte que garantizara su funcionamiento continuo sin ningún tipo de inconveniente.

- ✓ La identificación y valoración de activos, amenazas y riesgos que se ha presentado en este trabajo se puede aplicar a cada uno de los procesos de la empresa permitiendo un aseguramiento de la información de una manera completa.

- ✓ Al realizar el levantamiento, evaluación y análisis de información sin la colaboración de las personas que conocen el proceso de forma completa, se pueden llegar a omitir procesos, activos, amenazas, riesgos y salvaguardas que como persona externa no puedo identificar; esto también genera que se dificulte la toma de decisiones ya que la evaluación es muy subjetiva.

- ✓ La selección de la metodología se baso en la facilidad con la que se recopilo la información de las mismas; es decir existen metodologías de todo tipo pero obtener su base de conocimiento implica tener que gastar en dinero o en algunos casos son metodologías que no están traducidas al idiomaespañol.

- ✓ COBIT Y MAGERIT fueron las metodologías que obtuvieron los puntajes más altos con una diferencia muy baja entre las dos. La selección de MAGERIT se determino porque es una metodología que se enfoca específicamente en la identificación y valoración de los riesgos en seguridad de la información, mientras que COBIT se enfoca más en los procesos y el adecuado control de proyectos de tecnología. Es decir COBIT abarca la parte de seguridad de la información de una manera global o general; MAGERIT lo hace con más profundidad.

- ✓ Para dar el servicio, la mesa de ayuda tecnológica depende en gran parte del trabajo en conjunto de los activos de tipo Software, hardware y equipamiento auxiliar.

- ✓ El personal es el que administra los activos de información sacándoles el mejor provecho y efectividad para conseguir atender la necesidad u objetivo principal.

- ✓ Se puede notar que en los activos del proceso de la mesa de ayuda las valoraciones de las dimensiones de seguridad son muy similares o parecidas, es decir para los activos de la mesa de ayuda es importante asegurar las tres dimensiones de seguridad confidencialidad, integridad y disponibilidad en conjunto para que el activo no pierda su valoración total del activo.

- ✓ Como el objetivo de la mesa de ayuda es prestar un servicio de soporte continuo a los usuarios del banco; esto hace que la integridad y disponibilidad de este activo de información sea valorado dentro del rango de daño importante a daño grave, es decir que debe estar completo y disponible la mayor parte de tiempo.

- ✓ El objetivo de prestar soporte en la mesa de ayuda en una gran parte depende del personal y es por esto que la valoración de este activo de información es la más alta, sin incluir la confidencialidad que no se valora en este tipo de activo.

- ✓ Las salvaguardas que en el proceso de mesa de ayuda se aplican de manera preventiva permiten que los riesgos no pasen a un nivel alto, estas salvaguardas como lo son las capacitaciones al personal o la correcta definición de contratos con acuerdos de niveles de servicio son básicas y no generan mayor costo para la organización si se tiene en cuenta que la solución a un incidente puede generar impactos económicos severos.

- ✓ Las salvaguardas que se proponen son salvaguardas que no exigen de un gasto económico representativo, además son las salvaguardas más comunes y normales que debe tener cualquier proceso.

RESULTADOS

Resultados de la tabla de identificación de activos de la mesa de ayuda.

- ✓ La tabla arrojo la identificación de 15 activos de información, son pocos activos en comparación a los activos que se podrían identificar en otro proceso de la organización.

- ✓ Existe igual número de activos (3) para los tipos de activos de Datos / Información, Aplicaciones informáticas, Equipos Informáticos y Equipamiento Auxiliar; solo con la identificación no se puede determinar qué grupo de activos son los que requieren de un seguimiento mayor; esto hace necesario la valoración de los mismos.

- ✓ El único activo de Servicios es el soporte, lo que da a entender que la función principal de la mesa de ayuda es prestar un servicio como es el soporte tecnológico.

Resultados de la tabla de valoración de activos de mesa de ayuda.

- ✓ El activo con la valoración total más alta (27) es el servidor de base de datos y herramienta web; su valoración alta está definida ya que es el medio contenedor de la información del proceso.

- ✓ El activo con la valoración total más baja (9) es la aplicación para conexión remota; su valoración baja se da por que este activo no es determinante dentro del proceso de la mesa de ayuda, es decir su ausencia no genera retrasos ni la inactividad del proceso.

Resultados de la tabla de identificación y valoración de amenazas.

- ✓ La amenaza que más se presenta en los activos de información de la mesa de ayuda es “Avería de origen físico o lógico”; amenaza que se presenta por los defectos propios de origen o sobrevenida durante el funcionamiento del sistema, por esta razón se presenta en los activos de software, hardware, equipamiento auxiliar y redes de comunicaciones.

- ✓ El tipo de activo que tiene el mayor número (8) de amenazas es el hardware; esto permite ver que los activos físicos por sus características propias están expuestos a una mayor cantidad de amenazas.

- ✓ El tipo de activo que menos presenta amenazas es el “servicio”; esto representa un punto a favor para el proceso de mesa de ayuda ya que el

soporte brindado es el objetivo principal de la mesa de ayuda y demuestra la calidad del servicio que se está brindando.

- ✓ En la mayoría de activos se presenta una frecuencia baja en la que las amenazas se materializan, sin embargo el impacto que puede ocasionar esta materialización esporádica de la amenaza si puede llegar a detener la prestación del servicio de la mesa de ayuda porque su impacto si es alto.

Resultados de la tabla de identificación y valoración de riesgos.

- ✓ El riesgo con la valoración más alta (405) es la No disponibilidad del servidor de Base de datos y herramienta web; esto concuerda con ser el activo con la valoración más alta y con ser el medio contenedor de la información del proceso como ya se había mencionado.

- ✓ Los riesgos que pueden llegar a generar un impacto alto a nivel de credibilidad e imagen son los riesgos que como lo son el robo, robo de información o destrucción de información; pero al revisar la tabla son riesgos que están dentro del nivel bajo y esto genera confianza del proceso frente a la organización.

- ✓ Los activos de tipo aplicaciones informáticas (SW) son los activos con los riesgos más bajos.

- ✓ Los activos de tipo equipos informáticos (HW) son los activos con los riesgos más altos.

- ✓ La mayoría de riesgos de los activos de la mesa de ayuda se mantienen como riesgos bajos y medios; en donde solamente se debe mantener los controles que ya existen o reforzarlos.

Resultados de la tabla de identificación y valoración de salvaguardas.

- ✓ El riesgo generado de las amenazas se logro disminuir mediante las salvaguardas aplicadas a un nivel bajo que permitió asumirlo como un riesgo residual.

- ✓ Las salvaguardas que se proponen para los riesgos que existen permiten llevarlos a un nivel bajo de riesgo residual, en este caso es mucho más fácil asumir el riesgo, sin tener que llegar a transferirlo a un tercero.

BIBLIOGRAFÍA

Alberts, Christopher, etal.Introduction to the OCTAVE® Approach. Carnegie Mellon University, 2003.

COBIT.ControlOBjectives for Information and related Technology.ISACA [on line].Bogotá. Colombia [fecha de consulta: 10 de Noviembre de 2011]. Disponible en www.isaca-bogota.net/metodologias/cobit.aspx

COBIT 4.1.Control OBjectives for Information and related Technology.Resumenejecutivo.ISACA [on line].Bogotá. Colombia [fecha de consulta: 10 de Junio de 2011]. Disponible en www.isaca-bogota.net/metodologias/cobit.aspx

Definición de método inductivo.[on line]. [Fecha de consulta: 10 de Noviembre de 2011]. Disponible en http://definicion.de/metodo-inductivo/

Introductionto COBRA[on line].[Fecha de consulta: 10 de Noviembre de 2011]. Disponible en http://www.security-risk-analysis.com/introcob.htm

LACHEROS, Yanet Mejia. Investigación I. Colombia: Especialización en seguridad informática, 2010 42 p.

MATALOBOS VEIGA, Juan Manuel. Análisis de riesgos de seguridad de la información. Madrid: Universidad Politécnica de Madrid. Facultad de informática, 2009. 88 p.

MATALOBOS VEIGA, Juan Manuel. Análisis de riesgos de seguridad de la información. Madrid: Universidad Politécnica de Madrid. Facultad de informática, 2009. 107 p

MATALOBOS VEIGA, Juan Manuel. Análisis de riesgos de seguridad de la información. Madrid: Universidad Politécnica de Madrid. Facultad de informática, 2009. 108 p

MATALOBOS VEIGA, Juan Manuel. Análisis de riesgos de seguridad de la información. Madrid: Universidad Politécnica de Madrid. Facultad de informática, 2009. 109 p

Mesa de ayuda. [on line]. [Fecha de consulta: 10 de Noviembre de 2011]. Disponible en http://aceproject.org/main/espanol/et/etd04e.htm

MINISTERIO DE ADMINISTRACIONES PÚBLICAS. Metodología de Análisis y gestión de riesgos de los sistemas de información. Madrid, 2006. 17 p

MINISTERIO DE ADMINISTRACIONES PÚBLICAS. Metodología de Análisis y gestión de riesgos de los sistemas de información – Libro II. Catalogo de elementos. Madrid, 2006. 20 p.

MINISTERIO DE ADMINISTRACIONES PÚBLICAS. Metodología de Análisis y gestión de riesgos de los sistemas de información – Libro II. Catalogo de elementos. Madrid, 2006. 27 p.

MINISTERIO DE ADMINISTRACIONES PÚBLICAS. Metodología de Análisis y gestión de riesgos de los sistemas de información – Libro II. Catálogo de elementos. Madrid, 2006. 48 p.

OCTAVE Method Implementation Guide.Carnegie Mellon University [on line].Pittsburgh Pensilvania.[fecha de consulta: 9 de Junio de 2011]. Disponible en www.cert.org/octave/octavemethod.html

Portal Administración Electrónica. Centro de Transferencia de Tecnología – CTT. MAGERIT versión 2. [on line]. Madrid España.[fecha de consulta: 13 de Junio de 2011]. Disponible en http://administracionelectronica.gob.es.

¿Qué es una metodología?[on line]. [Fecha de consulta: 10 de Noviembre de 2011]. Disponible en http://www.misrespuestas.com/que-es-una-metodologia.html

VALENCIA, Alfonso. Presentación Gestión de la seguridad informática. Bogotá. Universidad Piloto de Colombia, 2010. 44 p.

GLOSARIO

Activo: Elementos que tienen valor para la organización.

Activos De Información: Según el ISO 17799:2005 (Código de práctica para la gestión de la seguridad de Información), un activo de información es “algo a lo que una organización directamente le asigna un valor y, por lo tanto, la organización debe proteger”. Algunos de estos activos son ficheros y bases de datos, documentación del sistema, manuales de usuarios, material de formación, procedimientos operativos o de soporte, planes de continuidad, configuración del soporte de recuperación, información archivada.

Amenaza: Causa potencial de un incidente no deseado, que puede ocasionar un daño a un sistema u organización.

Confidencialidad: Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.

Disponibilidad: Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada.

Incidente: Circunstancia o evento que sucede de manera inesperada y que puede afectar al desarrollo de un asunto o negocio, aunque no forme parte de él.

Información: es un conjunto organizado de datos procesados, que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje.

Integridad: Propiedad de salvaguardad la exactitud y estado completo de los activos.

Impacto: Medida del daño sobre el activo derivado de la materialización de una amenaza.

Metodología: conjunto de procedimientos basados en principios lógicos, utilizados para alcanzar una gama de objetivos que rigen en una investigación.

Riesgo: Combinación de la probabilidad de un evento y sus consecuencias.

Riesgo residual: es el riesgo remanente que existe después de que se hayan tomado las medidas de seguridad

Salvaguardas: Una salvaguarda o contramedida es cualquier cosa que ayuda a detener las amenazas sobre nuestros activos, Procedimiento o mecanismo tecnológico que reduce el riesgo.