CENTRO DE CIENCIAS BÁSICAS

DEPARTAMENTO DE SISTEMAS DE INFORMACION

TESIS

DISEÑO Y EVALUACIÓN DE UN PROCESO DE GESTIÓN DE SEGURIDAD DE SERVICIOS DE TI: CASO LABDC-UAA

PRESENTA

Ing. David Alejandro Montoya Murillo

PARA OBTENER EL GRADO DE MAESTRÍA EN INFORMÁTICA Y TECNOLOGÍAS COMPUTACIONALES

TUTOR

Dr. en Ing. José Manuel Mora Tavarez

COMITÉ TUTORAL

Dr. Jorge Marx Gómez, Universidad de Oldenburg, Alemania (co-director)

MC. Jorge Eduardo Macías Luévano, UAA

Aguascalientes, Ags., 31 de Mayo del 2016

UNIVERSIDAD AUTONOMA
DE AGUASCALIENTES

DAVID ALEJANDRO MONTOYA MURILLO
MAESTRÍA EN INFORMÁTICA Y TECNOLOGÍAS COMPUTACIONALES
P R E S E N T E.

Estimado alumno:

Por medio de este conducto me permito comunicar a Usted que habiendo recibido los votos aprobatorios de los revisores de su trabajo de tesis y/o caso práctico titulado: **"Diseño y evaluación de un proceso de gestión de seguridad de servicios de TI: Caso LABDC-UAA",** hago de su conocimiento que puede imprimir dicho documento y continuar con los trámites para la presentación de su examen de grado.

Sin otro particular me permito saludarle muy afectuosamente.

A T E N T A M E N T E
Aguascalientes, Ags., a 30 de mayo de 2016
"Se lumen proferre"
EL DECANO

M. en C. JOSE DE JESUS RUIZ GALLEGOS

c.c.p.- Archivo.

UNIVERSIDAD AUTONOMA DE AGUASCALIENTES

FORMATO DE CARTA DE VOTO APROBATORIO

M. EN C. JOSÉ DE JESÚS RUIZ GALLEGOS.
DECANO (A) DEL CENTRO DE CIENCIAS BÁSICAS

P R E S E N T E

Por medio del presente como Tutor designado del estudiante **DAVID ALEJANDRO MONTOYA MURILLO** con ID 129369 quien realizó la tesis titulado: **DISEÑO Y EVALUACIÓN DE UN PROCESO DE GESTIÓN DE SEGURIDAD DE SERVICIOS DE TI: CASO LABDC-UAA**, y con fundamento en el Artículo 175, Apartado II del Reglamento General de Docencia, me permito emitir el **VOTO APROBATORIO**, para que el pueda proceder a imprimirla, y así como continuar con el procedimiento administrativo para la obtención del grado.

Pongo lo anterior a su digna consideración y sin otro particular por el momento, me permito enviarle un cordial saludo.

A T E N T A M E N T E
"Se Lumen Proferre"
Aguascalientes, Ags., a 25 de Mayo de 2016.

Dr. José Manuel Mora Tavarez
Tutor de Tesis

c.c.p.- Interesado
c.c.p.- Secretaría de Investigación y Posgrado
c.c.p.- Jefatura del Depto. de Sistemas Electrónicos
c.c.p.- Consejero Académico
c.c.p.- Minuta Secretario Técnico

UNIVERSIDAD AUTONOMA DE AGUASCALIENTES

FORMATO DE CARTA DE VOTO APROBATORIO

M. EN C. JOSÉ DE JESÚS RUIZ GALLEGOS.
DECANO (A) DEL CENTRO DE CIENCIAS BÁSICAS

P R E S E N T E

Por medio del presente como Integrante del Comité Tutorial designado del estudiante **DAVID ALEJANDRO MONTOYA MURILLO** con ID 129369 quien realizó la tesis titulado: **DISEÑO Y EVALUACIÓN DE UN PROCESO DE GESTIÓN DE SEGURIDAD DE SERVICIOS DE TI: CASO LABDC-UAA**, y con fundamento en el Artículo 175, Apartado II del Reglamento General de Docencia, me permito emitir el **VOTO APROBATORIO**, para que el pueda proceder a imprimirla, y así como continuar con el procedimiento administrativo para la obtención del grado.

Pongo lo anterior a su digna consideración y sin otro particular por el momento, me permito enviarle un cordial saludo.

A T E N T A M E N T E
"Se Lumen Proferre"
Aguascalientes, Ags., a 25 de Mayo de 2016.

J. Marx Gómez

Dr. Jorge Marx Gómez
Integrante del Comité Tutorial

c.c.p.- Interesado
c.c.p.- Secretaría de Investigación y Posgrado
c.c.p.- Jefatura del Depto. de Sistemas Electrónicos
c.c.p.- Consejero Académico
c.c.p.- Minuta Secretario Técnico

UNIVERSIDAD AUTONOMA DE AGUASCALIENTES

FORMATO DE CARTA DE VOTO APROBATORIO

M. EN C. JOSÉ DE JESÚS RUIZ GALLEGOS.
DECANO DEL CENTRO DE CIENCIAS BÁSICAS
P R E S E N T E

Por medio del presente como Integrante del Comité Tutorial designado del estudiante **DAVID ALEJANDRO MONTOYA MURILLO** con ID 129369 quien realizó la tesis titulado: **DISEÑO Y EVALUACIÓN DE UN PROCESO DE GESTIÓN DE SEGURIDAD DE SERVICIOS DE TI: CASO LABDC-UAA**, y con fundamento en el Artículo 175, Apartado II del Reglamento General de Docencia, me permito emitir el **VOTO APROBATORIO**, para que el pueda proceder a imprimirla, y así como continuar con el procedimiento administrativo para la obtención del grado.

Pongo lo anterior a su digna consideración y sin otro particular por el momento, me permito enviarle un cordial saludo.

A T E N T A M E N T E
"Se Lumen Proferre"
Aguascalientes, Ags., a 25 de Mayo de 2016.

MC. Jorge E. Macías Luévano
Integrante del Comité Tutorial

c.c.p.- Interesado
c.c.p.- Secretaría de Investigación y Posgrado
c.c.p.- Jefatura del Depto. de Sistemas Electrónicos
c.c.p.- Consejero Académico
c.c.p.- Minuta Secretario Técnico

Agradecimientos

En el presente trabajo de Tesis antes que nada le agradezco a Dios por permitirme lograr llegar a donde estoy y darme las oportunidad que me a dado. Con estas palabras deseo expresar de corazón, de una forma profunda y sincera los agradecimientos a todas aquellas personas que colaboraron con la realización del presente trabajo de Tesis, un agradecimiento especial para el Dr. José Manuel Mora Tavarez, mi Director de Tesis, por su orientación, supervisión y seguimiento , pero sobre todo por la motivación, paciencia y principalmente el apoyo que me otorgo a lo largo de estos años. Sin duda alguna no pude haber elegido mejor opción como director de mi tesis. También agradezco su colaboración y apoyo a mis los integrantes de mi comité tutorial al M. en C. Jorge Eduardo Macías Luévano de la UAA y al Dr. Jorge Marx Gómez de la Universidad de Oldenburg en Alemania, sin olvidar el apoyo que me otorgo para lograr mi estancia en la Universidad de Oldenburg una experiencia olvidable.

Así mismo, quiero agradecer a la Universidad Autónoma de Aguascalientes por ofrecer posgrados de tan alta calidad como este y darme la oportunidad de formar parte de la Maestría en Informática y Tecnologías Computacionales.

De igual forma agradezco al Consejo Nacional de Ciencia y Tecnología (CONCAYT) por haberme brindado su apoyo a través de la beca para estudiantes de posgrados PNPC y permitirme formar parte del selecto grupo de becarios CONACYT.

Son muchas las personas que han formado parte de mi vida profesional que de una u otra forma me impulsaron a seguir adelante y que me encantaría agradecerles su amistad, consejos, apoyo, animo y compañía en los momentos más difíciles de mi vida. A mis compañeros y profesores por permitirme compartir con ellos este tiempo.

Y por ultimo quiero agradecer a mi familia, por estar todo el tiempo a mi lado, a mis hermanos y mi madre por confiar en mi, a mi novia por su apoyo y ayuda incondicional en el trayecto de estos años. Los quiero y les agradezco.

Dedico esta tesis a mis dos grandes maestros de la vida mi hermano y mi mama, quienes me han ensañado que si luchas por lo que quieres no hay imposibles y solo existen los limites que uno mismo se pone.

Índice General

Índice de tablas

Índice de figuras

Acrónimos

CCB Consejo de Coordinación de Empresas

CIS Elementos de la Configuración (por sus siglas en inglés Configuration Items)

CMBD Base de Datos de Gestión de Configuraciones (por sus siglas en inglés Configuration Management DataBase)

CMMI Integración de modelos de madurez de capacidades (por sus siglas en inglés Capability Maturity Model Integration)

COBiT Objetivos de control para la información y tecnologías relacionadas (por sus siglas en inglés Control Objetives for IT and related Technology)

CRAMM por sus siglas en inglés CCTA Risk Analysis and Management Method

DBMS Sistemas de Gestión de Bases de Datos (por sus siglas en inglés Database Management System)

DML La Biblioteca de Medios Definitivos (por sus siglas en inglés Definitive Media Library)

ICT por sus siglas en inglés information and communications technology

IDEF0 Definición de la integración para la modelización de las funciones (por sus siglas en inglés Integration Definition for Function Modeling)

IDS Sistema de detección de intrusos (por sus siglas en inglés Intrusion Detection System)

IEC Comisión Electrotécnica Internacional (por sus siglas en inglés International Electrotechnical Commission)

ISO Organización Internacional de Normalización (por sus siglas en inglés International Organization for Srandarization)

IT o TI Tecnologías de la Información

ITL Biblioteca de Infraestructura de Tecnologías de Información (por sus siglas en inglés Information Techology Infrastructure Library)

ITSM Gestión de servicios de tecnologías de la información (por sus siglas en inglés IT Service Managment)

LAN Red de área local (por sus siglas en inglés Local Area Network)

LTI Licenciatura en tecnologías de la información

MITC Maestría en informática y tecnologías de la computación

MOF por sus siglas en inglés Microsoft Operations Framework

MVSE Empresas mexicanas muy pequeña (por sus siglas en inglés Mexican Very Small Enterprises)

PYMES Pequeñas y Medianas Empresas

SADT Análisis Estructurado y Técnicas de Diseño (por sus siglas en inglés Structured Analysis and Design Technique)

SGSI Sistemas de Gestión de la Seguridad de la Información

SLA por sus siglas en inglés Service Level Agreement

Resumen

En la actualidad, la infraestructura de tecnologías de la información (TI) se ha convertido en esencial para las organizaciones, para prestar servicios de calidad a sus usuarios, mediante la cual, las organizaciones están buscando implementar normas que les permitan una mejor gestión de sus recursos, ya sea infraestructura o software, para aumentar la calidad de sus servicios y convertir esto en una ventaja competitiva en su campo. Debido a esto, es común el uso de ITSM (IT Service Management), que se basa en varios estándares, tales como: COBIR, MOF, ISO / IEC 20000 y ITIL, entre otros. En esta transición de proveedor de tecnología para el proveedor de servicios requiere el apoyo de estas metodologías. En este trabajo, se presenta un estudio sobre las metodologías ITIL v2, v3 MOF e ISO 20000, centrándose en el proceso de gestión de la seguridad en cada una de ellas, con el objetivo de diseñar un Proceso de Gestión de la Seguridad de Servicios de TI basado en las mejores prácticas de la norma ISO 20000, complementado con específica propuestas de MOF e ITIL v3 v2. Del mismo modo, la aplicación de este proceso en el caso de LabDC-UAA, que es, el laboratorio del Centro de Datos del Departamento de Sistemas Electrónicos de la Universidad Autónoma de Aguascalientes, e incluye unos 90 artículos en su infraestructura, además, cuenta con 28 servicios académicos que se ofrecen tanto a los alumnos como a los profesores de carreras relacionadas con TI. Esta situación hace necesaria la implementación de métodos de control, también, incluye el estudio de 3 herramientas de código abierto para apoyar el proceso de implementación. Del mismo modo, se somete a un proceso de evaluación mediante un par de cuestionarios que se puede ver en el Capítulo VII de este trabajo, en el que se recogieron los datos demográficos de los encuestados, y de la metodología propuesta se evalúan: constructos de utilidad, la facilidad de uso, compatibilidad, creencias normativas y la actitud final. Con el apoyo de los resultados de la evaluación, se puede concluir que la metodología propuesta en este trabajo para la implementación del proceso de gestión de la seguridad, con el apoyo de la herramienta de código abierto seleccionado (ProAct®), es

percibido por la gente como bastante útil, compatible con sus formas y necesidades de trabajo, y es coherente con los principios y comportamientos de trabajo de sus organizaciones, es decir, proporcionan beneficios a las organizaciones. Sin embargo, como con cualquier nuevo proceso organizacional para ser implementado, se identificó la necesidad de un período de entrenamiento, para utilizarlo correctamente. Por lo tanto, esta tesis, contribuye al avance del proceso de gestión del centro de datos de laboratorio para las organizaciones pequeñas o medianas, donde los altos costos impedían la adquisición de herramientas ITSM comerciales y contratar costosos consultores ITSM, a través de la provisión de un proceso esencial de gestión de seguridad, apoyado por una herramienta de código abierto.

Abstract

Currently, the information technology infrastructure (IT) has become essential for organizations, to deploy quality services to its users, whereby, organizations are looking to implement standards to enable them improved management of its resources, either infrastructure or software, to increase the quality of their services and turn this into a competitive advantage in their field. Because of this it is common to use ITSM (IT Service Management), which is based on several standards, such as: COBIR, MOF, ISO / IEC 20000 and ITIL, among others. In this transition from technology provider to service provider requires the support of these methodologies. This paper, presents a study about methodologies ITIL v2, MOF v3 and ISO 20000, focusing on the safety management process in each of them, with the aim of designing a IT Service Safety Management Process based on best practices of ISO 20000, supplemented with specific proposals from MOF and ITIL v3 v2. Likewise, the application of this process in the case of LabDC-UAA, which is, the Data Center Electronic Systems Department laboratory from Autonomous University of Aguascalientes, and includes about 90 items in its infrastructure, It also has 28 academic services offered to both students and teachers of IT careers. This situation makes it necessary to implement control methods, also, includes the study of 3 open source tools to support the implementation process. Similarly, it is subjected to an evaluation process by a pair of questionnaires that can be seen in Chapter VII of this work, in which the demographics of respondents were collected, and from the proposed methodology are evaluated: constructs of utility, ease of use, compatibility, normative beliefs and final attitude. With support from the results of the assessment, it can be concluded that the methodology proposed in this paper for implementation of safety management process, with the support of the selected open source tool (ProAct), is perceived by people as quite useful, compatible with its ways and needs of work, and it is consistent with the principles and behaviors of work of their organizations, ie, provide benefits to organizations. However, as with any new organizational process to be implemented, the need for a training period was

identified, to use it properly. Therefore, this thesis, contributes to the advancement of management process Laboratory Data Center for small organizations or medium, where high costs prevented the acquisition of commercial ITSM tools and hiring expensive consultants ITSM, through the provision of a essential security management process, supported by an open source tool.

I. Introducción

1.1 Contexto y Antecedentes Generales

Las organizaciones son más conscientes del papel esencial de la tecnología de la información (IT) dentro de las mismas, y se encuentran bajo presión para dar cuenta de los costos, y para gestionar los riesgos asociado con la creciente vulnerabilidad de su infraestructura de TI.

En las ultimas décadas las organizaciones o desarrolladores de (TI) han tenido un gran impacto en los procesos de negocios. La introducción de PC, LAN, la tecnología Cliente / Servidor y el internet ha permitido a las grandes organizaciones llevar sus productos o servicios a los mercados más rápidamente. Esto ha dado paso a la transición de la industria a la era de la información. En esta era todo es mas rápido y dinámico. Organizaciones jerárquicas tradicionales a menudo tienen dificultad para responder a los mercados, lo cual a provocado tendencias a cambios hacia ser menos jerárquica y lograr organizaciones flexibles(Cartlidge & LILLYCROP, 2004).

El creciente uso de las tecnologías de gestión de la información dentro de las empresas se ha traducido en las organizaciones de uso que dependen de TI que buscan tener servicios y soluciones tecnológicas cada vez más eficientes e innovadoras. Las organizaciones reconocen que los servicios de Tecnología de la Información (TI) son activos estratégicos para apoyar la gestión de la información y servicios. Sin embargo, la realidad es a menudo que estos servicios se pasan por alto o no se abordan en absoluto, con la importancia estratégica que conllevan (Lucio-Nieto, Colomo-Palacios, Soto-Acosta, Popa, & Amescua-Seco, 2012).

El término "servicios" es orientada a servicios asociados con los servicios Web y las arquitecturas. Durante la década de 1930, los EE.UU. Departamento de

Comercio acuñó el término "Servicio", usando tres secciones para describir la economía: agricultura, fabricación y servicio. Servicio, en ese momento, era un cajón de sastre para todas las actividades que no encajan en las otras dos categorías. Gestión de Servicios: la prestación de servicios y el servicio de apoyo, mejora de proceso tales como, Six Sigma, Gestión de Procesos de Negocio, y CMMI, (Galup, Dattero, Quan, & Conger, 2009).

"Un servicio es un medio para entregar valor a los clientes facilitándoles un resultado deseado sin la necesidad de que estos asuman los costes y riesgos específicos asociados." En otras palabras, el objetivo de un servicio es satisfacer una necesidad sin asumir directamente las capacidades y recursos necesarios para ello(Inform-IT, 2007, p. 3).

Actualmente, en México el Consejo de Coordinación de Empresas (CCB) [4] está promoviendo el uso de modelos y metodologías utilizados por grandes empresas con poca aceptación por MVSE debido a su complejidad y alta inversión en tiempo y recursos.(Fuentes-Penna, Díaz-Parra, Zavala-Díaz, Ruiz-Vanoye, & Olivares-Rojas, 2010)

En la gestión de servicio es un reto el entorno de sistemas distribuidos, porque todos los procesos deben proporcionar una prestación de servicios consistente, confiable y predecible. El marco de ITIL consiste en un bien evaluado, exploración y mantenimiento del conjunto de directrices (Talla, Valverde, Talla, & Valverde, 2013).

Para las TI la gestión de la misma se ha convertido en un punto muy importante para cualquier organización que desee prestar servicios de calidad y seguros a sus usuarios, por lo cual las organizaciones buscan lograr implementar estándares los cuales permitan mejorar la seguridad de sus servicios como dentro de la misma, para aumentar calidad en sus servicios y obtener una ventaja competitiva. Para lograr esto recurren a la Administración

de servicios de TI (iTSM: por sus siglas en ingles IT Service Managment) el cual esta basado en ITIL.

ITIL (Information Techology Infrastructure Library, proporciona un marco de orientación de las "mejores prácticas" para la gestión de servicios y es el método más ampliamente utilizado y aceptado para la Gestión de Servicios en el mundo, desarrollado por el gobierno de Reino Unido en 1980, quien impulsado por la necesidad de la mejora de eficiencia, se decidió a documentar el como las mejores y mas exitosas empresas u organizaciones aplicaban la gestión de servicios. A finales de 1980 y principios de 1990, se habían producido una serie de libros los cuales documentaban un acercamiento a la gestión de servicios de TI necesarios para apoyar a los usuarios de negocios. ITIL proporciona una descripción detallada de una serie de prácticas de TI importantes, con amplias listas de control, tareas, procedimientos y responsabilidades que pueden adaptarse a cualquier organización de TI. Siempre que sea posible, estas prácticas se han definido como procesos que cubren las principales actividades de TI organizaciones de servicios. La amplia área temática cubierta por las publicaciones de ITIL hace útil para referirse a ellos con regularidad y usarlos para establecer nuevos objetivos de mejora para la organización de TI. La organización puede crecer y madurar con ellos (ITIL). (Cartlidge & LILLYCROP, 2004)

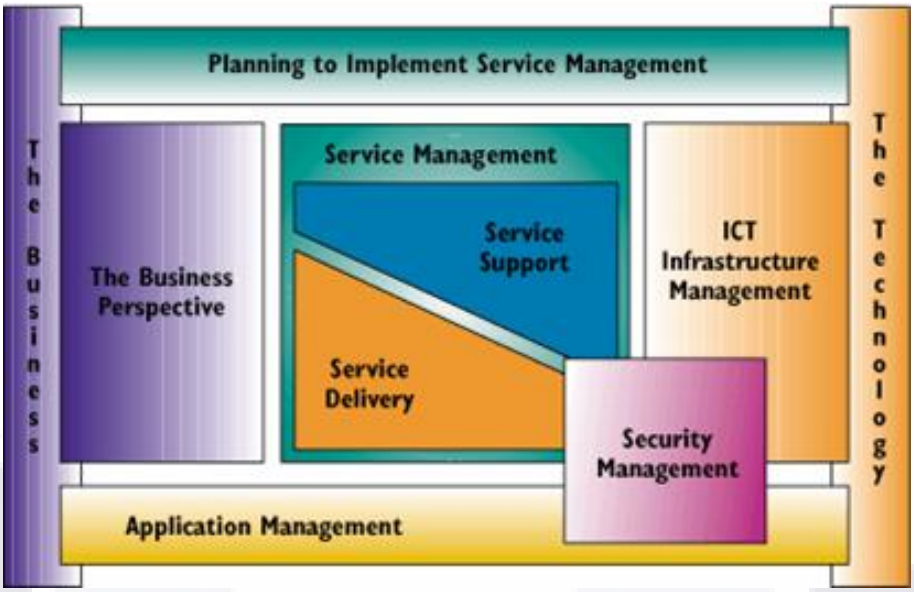


Figura 1 Marco global de ITIL (tomado de ITIL)

ITIL facilita que las empresas transformen sus áreas de TI de un proveedor de tecnología tradicional aun proveedor de servicios confiable y de bajo costo (Ying, Lijun, & Wei, 2009).

El marco de mejores prácticas de ITIL permite a los responsables documentar, auditorías y mejorar su servicio de TI en los procesos de gestión. Sin embargo, hasta la fecha, ha habido investigación académica limitada acerca de la adopción de ITIL (Hochstein, Tamm, & Brenner, 2005).

Este enfoque a servicios al que se están moviendo las organizaciones da pie a pensar: ¿Qué es un servicio? Un servicio constituye un medio de proporcionar valor al usuario al facilitar los resultados que desean alcanzar los usuarios sin la necesidad de que asuman los costos y riesgos específicos asociados (ITIL v3, 2007).

Se encontró que tanto la satisfacción del cliente y el rendimiento operativo mejoran a medida que las actividades en el marco ITIL . El aumento en el uso de ITIL, es probable que resulte en mejoras en la satisfacción del cliente y el rendimiento operativo (Potgieter, Botha, & Lew, 2005).

Debido ITSM es centrada en el proceso, que comparte un tema común con el movimiento de mejora de procesos (tales como, Six Sigma, Gestión de Procesos de Negocio, y CMMI). ITSM ofrece un marco para alinear las operaciones de TI relacionados con las actividades y las interacciones de TI de personal técnico con las empresas, clientes y procesos. La evolución de los estándares de mejores prácticas de ITSM empezando por el de ITIL y más recientemente, la Organización Internacional de Normalización (ISO) en diciembre del 2005 / Comisión Electrotécnica Internacional (IEC) estándar 20000, así como las demás normas (tales como, COBIT, etc.) que influyeron en la creación de la norma ISO / IEC 20000.(Cartlidge & LILLYCROP, 2004)

Aunque existen diferentes marcos de administración de servicios de TI que una organización puede utilizar como son: Objetivos de control para TI y tecnología relacionada (COBIT, de sus siglas en ingles: Control Objetives for IT and related Technology), Marco de Operaciones Microsoft (MOF, de sus siglas en inglés: Microsoft Operations Framework), Estándar de administración de servicios de TI ISO/IEC 20000 (International Organization for Standardization/ International Electrotechnical Commission 20000), y la Biblioteca de Infraestructura de TI (ITIL de sus siglas en ingles: Information Technology Infraestructure Library), por mencionar algunos.

1.2 Data Center LabDC-UAA

De manera general el Laboratorio del Data Center de la Universidad Autónoma de Aguascalientes (LabDC-UAA), es un laboratorio destinado a proporcionar servicios de TI para la carrera de Licenciado en tecnólogas de la información (LTI) y la Maestría en Informática y Tecnologías Computacionales (MITC). Así mismo su planeación, diseño, autorización de recursos financieros, instalación y puesta en marcha ocurrió de Enero 2011 a Julio 2012.
Acorde a Documentos de Diseño del Laboratorio (Mora et al. 2012), el objetivo del Proyecto se estableció como:

- *Contar con una Laboratorio Avanzado de Informática de tipo Data Center para apoyar las actividades de Docencia de Cursos pertinentes de la Carrera de LTI y de la Maestría MITC, así como Proyectos de Investigación en Gestión en Ingeniería de Servicios de TI.*

Así mismo, se plantearon los siguientes objetivos específicos (Mora et al. 2012):

- *Objetivo 1: contar con un ambiente avanzado (LabDC-UAA) de Gestión de Servicios de TI que permita la docencia de cursos especiales de la Maestría en Informática y Tecnologías Computacionales, y de la Lic. en TI (cursos de Gestión de TI, 10º semestre y curso optativo de Taller de Gestión de Servicios de TI).*
- *Objetivo 2: contar con un ambiente avanzado (LabDC-UAA) de Gestión de Servicios de TI que permita la Investigación en la Ingeniería y la Gestión de Servicios de TI de Nivel Maestría y Doctorado, así como Proyectos adicionales.*
- *Objetivo 3: contar con un ambiente avanzado (Laboratorio Data Center) de Gestión de Servicios de TI que apoye la realización de Practicas de Becarios de MITC, Practicas Profesionales y de Servicio Social.*
- *Objetivo 4: contar con un ambiente avanzado (LabDC-UAA) de Gestión de Servicios de TI que permita la impartición de Cursos Cortos, Procesos y Herramientas de Gestión de Servicios de TI a la Industria.*

El laboratorio inició oferta de servicios de TI en Agosto 2012 con 14 servicios. En Enero 2013 se amplio a 28 servicios de TI.

Respecto al personal encargado, el laboratorio no cuenta con personal de tiempo completo. En Figura 1 se presenta el organigrama (Mora et al. 2012) planeado:

Figura 2 Organigrama (Mora et al 2012)

El organigrama planeado refleja un administrador general, 3 supervisores (investigación, operaciones y financiero) y 3 grupos de colaboración. Por restricciones de presupuesto, la operación real actual es la siguiente: 1 coordinador general (tiempo extra asignado), 1 Técnico de Apoyo como Soporte Técnico de 20 hrs/semana, 3 Becarios de MITC (de 10 hrs c/u x semana).

Así podemos plantear la siguiente pregunta, ¿Qué es un Data Center?, Un Data Center es una locación (1 oficina, 1 piso, o 1 área completa) de un edificio, acondicionado específicamente para alojar los equipos centrales de ICT de una organización. Por extensión, también se le considera al área general donde se ubica el Personal de Informática y Equipos de ICT adicionales. (Mora 2013). De acuerdo al curso de Administración de Data Centers del Dr. Mora, existe una clasificación de data centers como se observa a continuación:

Figura 3 Tipos de Data Center (Mora 2013), dicha clasificación es propuesta por America Power Conversion (APC)

De acuerdo a dicha clasificación por su nivel de criticidad, su descripción es la siguiente:

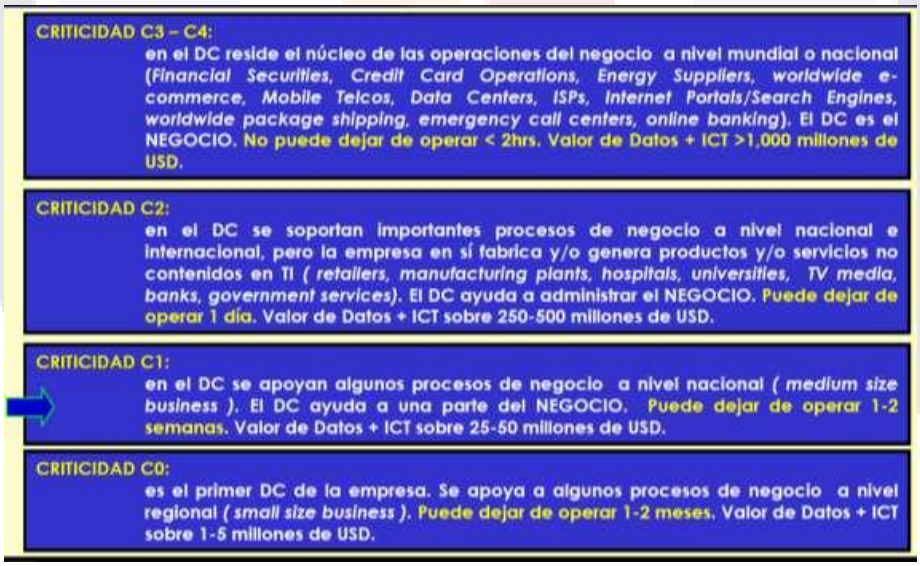


Figura 4 Nivel de de Criticidad del Data Center (Mora 2013), categoría adaptada del Curso de Data Centers 2013 por el Dr. Mora.

De acuerdo con la clasificación anterior el LabDC-UAA es de tipo C1 pequeño, sin embargo aunque no opera como un data center de una empresa mediana normal debido al contexto en que opera, la falta de recursos humanos de

tiempo completo y el limitado presupuesto destinado a su operación, gracias a la infraestructura que tiene (dos racks, cuatro servers, etc. (Figura 5))entra en esta clasificación.

1.3 Metodología del Caso de Estudio

Para la metodología se baso en trabajo del Dr. Manuel Mora T. llamado Descripción del Método de Investigación Conceptual: Tipo Conductual o Tipo Diseño (en su versión 3.5 de Agosto del 2009). Donde denota que un proceso de investigación científica puede ser dirigido por diversos métodos (Ackoff, 1962).

En el campo de los Sistemas de Información, han ávido diversos estudios que aportan evidencias de que el Método de Investigación Conceptual es considerado como parte importante del repertorio posible de los métodos de investigación disponibles en el área (Straub, Ang y Evaristo, 1994; Parker et al 1994; Vessey, Ramesh y Glass, 2002; Samuels y Steinbart, 2002).

En lo que concluyo el Dr. Mora en la investigación previamente mencionada fue:

Descripción del Método de Investigación Conceptual: Tipo Conductual o Tipo Diseño.

a) Fase I de Formulación del Problema de Investigación.

- a.1 Contexto y antecedentes generales del problema.
- a.2 Situación problemática.
- a.3 Tipo y Propósito de Investigación.
- a.4 Relevancia.
- a.5 Objetivos, preguntas e hipótesis/proposiciones de la investigación.

(b) Fase II de Análisis de Trabajos Relacionados.

b.1 Teorías Bases.
b.2 Estudios Relacionados.
b.3 Contribuciones y Limitaciones de Estudios Relacionados.
b.4 Selección/Diseño de Marco Conceptual General.
b.5 Selección/Diseño de Modelo de Investigación Particular.

(c) Fase III de Aplicación o Diseño de Modelo Conceptual.

c.1 Aplicación o Diseño Creativo-Racional-Deductivo de Modelo Conceptual.

(d)Fase IV de Validación del Modelo Conceptual Aplicado o Diseñado.

d.1 Validación de Contenido por Panel de Expertos.
d.2 Validación por Argumentación Lógica.
d.2 Validación por Prueba de Concepto de Construcción de Artefacto.
d.3 Validación por Estudio Piloto por Encuestas.

Con ayuda del mismo trabajo previamente mencionado y acompañado por la experiencia de tutores en área de tecnologías de la información y la investigación en esta área se determino escoger el diseño por un proceso de búsqueda Heurística para el proceso de diseño, por lo cual la búsqueda se realizo en el espacio de búsqueda de diseños posibles, mas no necesariamente cumpliendo todos los objetivos y restricciones de diseño fijadas, es por esto que soluciones viables son conservadas y no descartadas perpetuamente.

Respecto a la validación del modelo conceptual se determino el uso de la validez por Argumentación Lógica, la cual incluye demostración de teoremas como caso especial, donde se basa en la creación de argumentos lógicos, coherentes y teóricamente robustos para lograr soportar el modelo conceptual.

1.4 Relevancia de la investigación

A pesar de la popularidad de ITIL, ha habido poca investigación académica publicada hasta la fecha sobre cuestiones relacionadas con la adopción de ITIL e implementación. Muchas organizaciones del sector público y privado han adoptado ITIL y están haciendo progresos sustanciales en la aplicación del marco (Cater-Steel & Tan, 2005a). Grandes organizaciones, especialmente aquellas con una gran fuerza laboral de TI están liderando la implementación. Aunque todas las funciones y procesos de ITIL básicas están siendo implementadas (Cater-Steel & Tan, 2005b).

A través de investigación y análisis de la adopción de ITIL en grandes organizaciones, se ha explorado el impacto de la adopción de ITIL, la secuencia de selección de los procesos de ITIL, aplicar estrategias para gestionar la organización del cambio, el papel y el uso de herramientas de apoyo y tecnologías y los factores críticos de éxito y beneficios de adopción de ITIL. Esta considera los desafíos que enfrentan las organizaciones en su adopción de ITIL. Muchas organizaciones han informado de que no han progresado tanto como deseaban, debido a problemas como la falta de apoyo a la gestión, el cambio cultural en términos de resistencia por parte de personal técnico, y los retrasos en el establecimiento de un conjunto de herramientas apropiadas. "El punto de vista financiero es muy importante, pero demasiado limitado para el desempeño de gestión de servicios de TI" (Cater-Steel, Toleman, & Tan, 2006).

Hay un creciente reconocimiento de la necesidad de una amplia gama de normas de seguridad informática y directrices técnicas para apoyar la seguridad cibernética, tanto a nivel nacional como internacional. Tanto los gobiernos como el sector privado tienen un papel importante que desempeñar en el desarrollo, implementación y promoción de dichas normas.

En este contexto (Fumy, 2004) señala que "Inevitablemente, el establecimiento de normas de seguridad de tecnología de la información

significa ponerse al día con la tecnología y el ingenio de las personas que atacan a los sistemas de TI. Pero hay que hacerlo".

Sistemas, redes y políticas deben ser diseñadas adecuadamente, aplicarse y por ende optimizar la seguridad. La especificación y adopción de salvaguardas y soluciones (tanto técnicos como no técnicos) son apropiadas para evitar o limitar el daño potencial de las amenazas y vulnerabilidades identificadas. Afortunadamente, un número de estándares están disponibles o en desarrollo. También hay una continua necesidad de revisar las políticas, medidas y procedimientos para asegurar que cumplen con los cambiantes desafíos que plantean las amenazas a los sistemas de TI y redes. En el año 2006, no existía aun un sistema de gestión de seguridad de Sistemas de Gestión de la Seguridad de la Información (SGSI) estándar.

Los expertos coinciden en que el principal desafío para las empresas y el sector público de hoy no es la tecnología de seguridad en sí, sino la forma de establecer los procedimientos adecuados, la gestión y los controles para el logro de la seguridad informática (Doughty, 2003). Los seres humanos seguirán siendo menos fiables y menos fáciles de predecir. La formación y la educación, así como el apoyo y compromiso de la alta dirección continuarán siendo cuestiones clave.

La información es un activo esencial para las organizaciones, ya que apoya las operaciones del día de hoy y facilita la toma de decisiones de los actores clave de la organización. El desafío que enfrentan las organizaciones es cómo proporcionar acceso a este activo sin comprometer su integridad. Este activo es recibido y distribuido por la organización a través de diferentes canales de distribución, que se conectan entre sí por la red de las telecomunicaciones. Estos canales incluyen:

- Correo electrónico
- Internet

- Las aplicaciones (por ejemplo, Financiera, Logística, Inmobiliario y Construcción, Energía, etc.)
- DBMS (MS SQL Server, Oracle, DB2, Sybase, etc.)
- Los sistemas operativos (por ejemplo, Unix, NT / Windows 2000, etc.)

Aunque la piratería y los virus pueden ser considerados como la amenaza más inmediata y mayor a las organizaciones en la actualidad, existen riesgos de seguridad en otras áreas que a menudo no son tratados adecuadamente. La educación del personal en el control de la empresa y la información confidencial es un buen ejemplo (Doughty, 2003).

Según la encuesta de infracciones de la Seguridad de la Información 2002 (ISBS 2002) Dirigido por Pricewaterhousecoopers (PwC) en Reino Unido destacó que:

- 44% de las empresas del Reino Unido han sufrido al menos un fallo de seguridad malicioso en el año pasado.
- El costo promedio de un incidente de seguridad grave era £ 30 000. Varias empresas encuestadas tenían incidentes de seguridad de más de 500.000 libras esterlinas.
- 20% de las organizaciones grandes que tuvieron un incidente, tardaron más de una semana para volver a las operaciones normales del negocio.
- El 27% de quienes respondieron a la encuesta indicaron que tenían una política de seguridad documentada.
- Sólo el 15% de los encuestados indicaron que ellos estaban conscientes de la norma BS7799 de seguridad, que ha sido adoptada por la Organización Internacional de Normalización (ISO 17799)
- Sólo el 33% de los sitios web del Reino Unido tiene el software para detectar la intrusión. Sólo el 51% de los sitios web transaccionales pueden cifrar las transacciones que pasan a través de Internet.
- 19% de las organizaciones que proporcionan acceso remoto han implementado la autenticación de los factores.

La encuesta realizada en el año 2003 indico una vez más que la seguridad no está todavía siendo tratada por las organizaciones como una inversión en la protección de sus activos de información.
Las organizaciones invierten en medidas preventivas de seguridad para proteger sus activos de una violación de la confidencialidad, la integridad y la pérdida de calidad en los servicios (Abimbola, 2007).

Un hito de la norma Information Technology Infrastructure Library (ITIL) es el desarrollo de un modelo eficaz de gestión de incidentes. Asegura continuidad del servicio en relación con los cuatro elementos de la Tecnología de la Información de Gestión de Servicios de TI (ITSM): organización, personal, tecnologías y procesos. De acuerdo con las definiciones de ITIL más recientes, el objetivo principal de la gestión de incidentes es reducir al mínimo las interrupciones en las actividades empresariales y garantizar la disponibilidad del servicio. La experiencia en el campo sugiere que el enfoque de ITIL para la gestión de incidentes es exactamente lo que pretende ser: un apoyo a la prestación de servicios. Pero si nos fijamos en lo estrictamente desde el punto de vista de seguridad nos vemos obligados a considerar que es insuficiente en términos de coherencia y eficacia.

No obstante, es posible tomar los componentes del proceso de ITIL y utilizarlos para mejorar la gestión de incidentes de seguridad. Pero esta no es nuestra principal preocupación (Forte, 2007).

Por ello es que se puede ver que aunque la literatura actual cuenta con distintas investigaciones relacionadas con ITIL y en la gestión de seguridad no se tiene alguna versión simplificada para el método de la gestión de seguridad orientadas a organizaciones medias con data centers de niveles intermedios por lo cual la investigación de correlación de ITIL v2 , ITIL v3, MOF, CRAMM así como ISO 20000. Con un enfoque mas orientado al de estas organizaciones que no cuentan con un equipo el cual se pueda dedicar totalmente a la aplicación de los módulos de los distintas modelos o métricas.

El tener una mejor administración de los procesos realizados, incluyendo el proceso gestión de seguridad TI, permite tener control sobre posibles peligros o riesgos en la entrega de un servicio; inclusive se hace más fácil justificar la adquisición de nuevos dispositivos o software para su mejor control. El LabDC-UAA incluye en su infraestructura aproximadamente 90 elementos. Además de que cuenta con 28 servicios académicos que ofrece tanto a los alumnos como a los profesores de carreras relacionadas con TI, por esto se vuelve importante la investigación sobre estándares como ITIL e ISO/IEC 20000, dichos estándares contemplan dentro de sus procesos el proceso de Gestión de Seguridad, en el caso de ISO/IEC 20000 en la fase de Seguridad de la información, en ITIL v2 dentro de la fase de Gestión de Seguridad y al igual que en MOF v3. Teniendo en cuenta que este proceso podrá ser aplicado a otros data center de nivel C0 o C1 debido a que es uno de los puntos importantes de esta investigación poder crear un proceso de gestión de la seguridad aplicable a data centers de Pymes que no cuentan con algún tipo de control de seguridad en sus servicios de TI.

II. Formulación de Problema

2.1 Problema de investigación especifico

En un centro de información se cuenta con diversa infraestructura de hardware y software cuyo objetivo es proporcionar servicios de TI a distintos usuarios. Por lo que debemos tomar en cuenta que para que un servicio esté disponible es necesario tener control sobre los elementos que son requeridos para proporcionarlos, es aquí donde interviene el proceso de gestión de seguridad de TI. El proceso de gestión de seguridad de servicios de TI es algo complejo debido a la enorme cantidad de información que se debe recopilar y mantener actualizada así como los diferentes puntos que se tienen que cuidar para tener control de la seguridad de los servicios. Por lo que se vuelve indispensable contar con herramientas que facilite este proceso. Debido a esto se recurre a diferentes estándares como ITIL e ISO/IEC 20000, dichos estándares contemplan dentro de sus procesos el proceso de Gestión de Seguridad, en el caso de ISO/IEC 20000 en la fase de Seguridad de la información, en ITIL v2 dentro de la fase de Gestión de Seguridad y al igual que en MOF v3. Tomando en cuenta que las practicas de ITIL son tan solo una guía para la ayuda de las personas que intentan comprender los procesos principales y dejando la implementación de esta a los profesionales del área, es por ello que la implementación exige cambios profundos que afectan personas, procesos y tecnología. En muchas ocasiones gestionar la seguridad no se le da el valor que debería sin embargo una mala gestión de ella puede llevar a accidentes o pérdidas de la información lo que resultaría en un menor nivel de servicio de lo acordado con los clientes o incluso un costo mayor en el servicio. Esto implica que tener una buena gestión de seguridad de TI sea algo esencial e importante para garantizar la calidad de los servicios que se proporcionan.

Las personas encargadas de implantar dicho proceso, muchas veces encuentran que la herramienta usada para implantarlos no está alineada

totalmente con los requisitos planteados por los estándares para la gestión de seguridad de TI, por lo que mapear la información que se tiene con la herramienta disponible se vuelve un proceso difícil. Partiendo de este punto, se propondrá un proceso esencial de gestión de seguridad de servicios de TI apoyado en el uso de herramientas open source disponibles para su implantación.

En el caso especifico del Laboratorio LabDC-UAA, la problemática actual consiste en:

- Se percibe como necesario contar con un control de los elementos de seguridad de TI con que se cuenta ya que del control que se tenga sobre estos elementos depende la calidad de los servicios que se ofrecen.
- Adicionalmente se requiere de una herramienta que permita cubrir la gestión de este punto, que no genere gastos adicionales al LabDC-UAA, por lo que nos inclinaremos en una herramienta open source.

Esto debido principalmente a la no disponibilidad de recursos financieros para contar con personal de tiempo completo. También es positivo indicar que la demanda actual de servicios de TI instalados es aun baja, y esto se convierte en un círculo negativo: no se autoriza más personal ya que no se explotan todos los servicios de TI y viceversa. Sin embargo, los 28 servicios de TI están totalmente operativos y demandan un seguimiento básico como lo recomiendan las mejores practicas de ISO 20000, ITIL v2 e MOF v3. Así mismo, a pesar de la poca utilización, actualmente, la infraestructura de TI del Laboratorio demanda un proceso Esencial de Gestión de Seguridad de Servicios de TI. La siguiente figura reporta la Arquitectura general del LabDC-UAA.

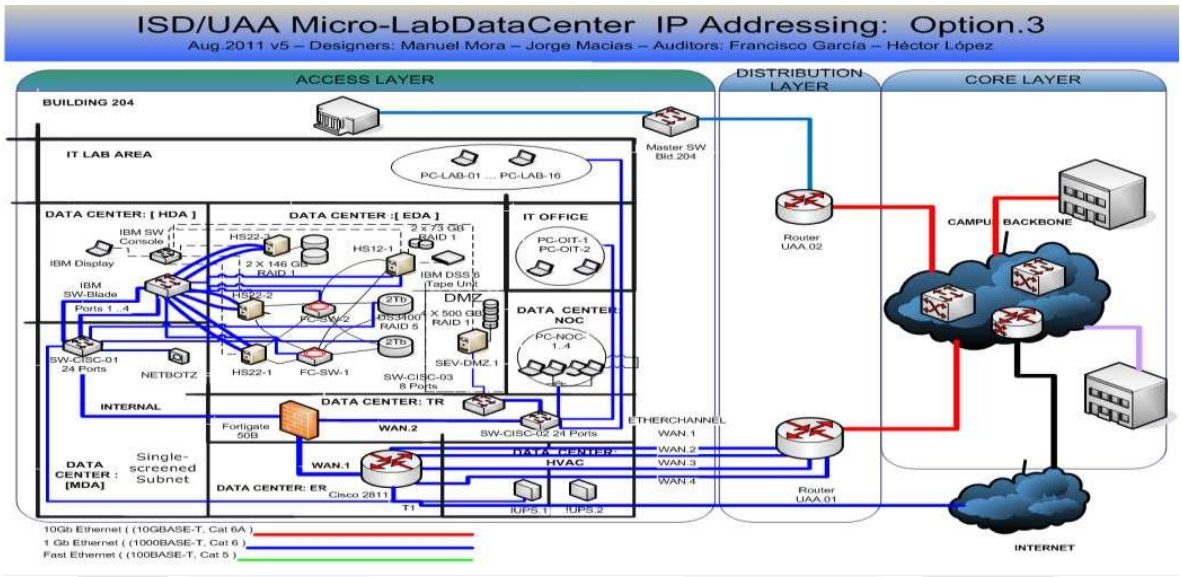


Figura 5 Arquitectura general del Laboratorio Data Center de la UAA (Diseño LabDC-UAA del Dr. Mora)

En resumen, en el plan inicial del Laboratorio se ha definido un Manual Básico de Política y Operaciones, que incluye las tareas de control de elementos de la infraestructura tanto Hardware como Software de manera general. Así mismo se han localizado herramientas open source que permiten llevar el registro general. Sin embargo, a la fecha no han sido implantados por la falta de definición de un proceso concreto que defina las tareas a realizar de manera detallada en el tema particular de Gestión de Seguridad en TI. Esta Tesis es desarrollada para ayudar en tal problemática.

2.2 Objetivos de la Investigación

2.2.1 Objetivo General

Diseñar y Evaluar (en modo piloto) un proceso adecuado de Gestión de Seguridad de Servicios de TI basado en las mejores prácticas de ISO 20000, complementados con propuestas particulares de ITIL v2 y MOF3 y soportado por una herramienta Open Source.

2.2.2 Objetivos Particulares

1. Estudiar la Fase de Gestión de Seguridad de la Información de ISO 20000, y los procesos asociados a tal fase en ITIL v2 y MOF v3.
2. Diseñar un Proceso de Gestión de Seguridad de Servicios de TI basado en (1) que sea adecuado (e.g. útil, fácil de usar, compatibilidad, creencias normativas y actitud final).
3. Seleccionar una herramienta open source para implantar el Proceso (al máximo posible según las capacidades de la herramienta).
4. Diseñar los instrumentos de evaluación del proceso de gestión de seguridad.
5. Evaluar la UTILIDAD, FACILIDAD DE USO, COMPATIBILIDAD, CREENCIAS NORMATIVAS Y ACTITUD FINAL percibidos sobre el Proceso diseñado y la herramienta open source de soporte por una muestra piloto de Profesionistas de TI de Data Centers similares al LabDC-UAA.

2.3 Preguntas de la Investigación

1. ¿Cuáles son los Procesos de Seguridad en servicios de TI propuestos en la Fase Procesos de Control en ISO 20000 y sus correspondencias de tales Procesos con los propuestos en ITIL v2 y MOF v3?
2. ¿Es factible generar un proceso de gestión de seguridad de servicios de TI basado en tales revisiones que sea percibido como adecuado (e.g. útil, fácil de usar, compatibilidad, creencias normativas y actitud final).
3. ¿Es factible soportar el Proceso diseñado con alguna de las herramientas open source disponibles?
4. ¿Cuáles son los valores obtenidos en los constructos de UTILIDAD, FACILIDAD DE USO, COMPATIBILIDAD, CREENCIAS NORMATIVAS, Y ACTITUD FINAL percibidos por una muestra piloto de Profesionistas

en TI de Data Centers similares al LabDC-UAA al evaluar El Modelo diseñado y la Herramienta de Soporte (si (3) es logrado)?

2.4 Hipótesis de la Investigación

H1.- La Fase de Procesos de Control de ISO 20000 tiene procesos para ser usados en un Diseño de un proceso de gestión de TI y existe correspondencia con procesos en ITIL v2 y MOF v3.

H2.- Un Proceso de gestión de seguridad de servicios de TI basado en ISO 20000 y complementado con los sub-procesos asociados de ITIL v2 e MOF v3 que sea adecuado es factible de ser diseñado.

H3.- El Proceso diseñado es factible de ser soportado con una herramienta open source.

H4.- Los valores obtenidos en los constructos de UTILIDAD, FACILIDAD DE USO, COMPATIBILIDAD, CREENCIAS NORMATIVAS Y ACTITUD FINAL percibidos por una muestra piloto de Profesionistas en TI de Data Centers similares al LabDC-UAA al evaluar el Modelo diseñado y la Herramienta de Soporte serán adecuados (valores mayores o iguales a 3.0 en un Escala de Likert de 1 a 5).

III. Marco Teórico

3.1 Gestión de Servicios de TI (ITSM)

El área de TI se ha vuelto un tema trascendente en cualquier organización debido a la importancia que esta a tomado, debido al rol tan importante que ha ido tomando para el apoyo y control de una buena gestión de los servicios que ofrece la organización logrando reducir costos, permitir una mejora del servicio logrando tener una ventaja competitiva.

Las áreas de TI de organizaciones mexicanas están cambiando el enfoque a ser proveedores de servicio de TI eficientes. Por lo cual para lograr este cambio están acudiendo a la Gestión de Servicios de TI (ITSM, de sus siglas e ingles : IT Service Management). ITSM se enfoca en la entrega y soporte de TI que son adecuados para los requerimientos de negocios de la organización y logra esto mediante el aprovechamiento de ITIL, que se basa en las mejores prácticas para promover la eficacia y eficiencia empresarial. (Ying, 2009).

La oportunidad de innovar en servicios, para realizar negocios y valor social a partir del conocimiento sobre el servicio, a la investigación, desarrollar y entregar nuevos servicios de información y servicios de negocios, nunca ha sido mayor (ITSM.2009.CACM). Existen diferentes marcos de gestión de servicios de TI que una organización puede usar como base para control de TI o tecnologías relacionadas como COBIT, de sus siglas en inglés: Control Objetives for IT and related Technology), Marco de Operaciones Microsoft (MoF, de sus siglas en inglés: Microsoft Operations Framework), Estándar de administración de servicios de TI ISO/IEC 20000 (International Organization for Standardization/ International Electrotechnical Commission 20000), y la Biblioteca de Infraestructura de TI (ITIL de sus siglas en inglés: Information Technology Infraestructure Library), por mencionar algunos.

Sin embargo, el más reconocido a nivel mundial es ITIL, del cual se revisará el proceso de Gestión de Seguridad de la versión 2 del libro, de igual forma se revisará la sección relacionada con Gestión de Seguridad del modelo MoF, con lo cual se permitirá identificar la correspondencia de estos procesos con los planteados en ISO/IEC 20000 para crear una comparación entre estos marcos de administración de TI que permitan comprender de manera más clara dichos procesos.

3.2 Proceso de Gestión de Seguridad (Security Management) en ITIL v2

La sección de Gestión de Seguridad en ITIL v2 es un módulo en particular con el nombre de Security Management (en el caso de ITIL v3 el termino Gestión de Seguridad es tratado dentro de la fase de Funciones y Procesos en Diseño del Servicio es por eso que se opto por usar ITIL v2).

3.2.1 La fase de Gestión de Seguridad (Security Management)

Una organización no debe funcionar sin un suministro controlado de información, Gestión de la seguridad de la Información es una actividad importante que apunta a controlar el suministro de información y para evitar el uso no autorizado de la información. Seguridad es ahora un aspecto esencial de calidad en la gestión de servicios.

Seguridad en ITIL se relaciona en parte con la administración de disponibilidad. Gestión de la seguridad se ha convertido en una cuestión importante en la moderna gestión de servicios de TI "Seguridad se refiere a no ser vulnerables a riesgos conocidos, desconocidos y evitar riesgos en la medida de lo posible"(Cartlidge & LILLYCROP, 2004).

ITIL maneja 3 conceptos fundamentales relacionados con la seguridad:

- **Confidencialidad**: protección de la información contra el acceso y el uso no autorizado.
- **Integridad**: exactitud y oportunidad de la información.
- **Disponibilidad**: la información debe ser accesible a cualquier hora acordada. Esto depende de la continuidad de los sistemas de tratamiento de la información.

Gestión de la seguridad tiene dos objetivos:

- Cumplir los requisitos de seguridad de nivel de servicio y las necesidades externas de los contratos, la legislación y las políticas impuestas desde el exterior.
- Para proporcionar un nivel básico de seguridad, independiente de requisitos externos.

3.2.2 Proceso de Gestión de Seguridad (Security Management)

Gestión de la seguridad de un ciclo interminable de planificar, desarrollar, controlar y actuar.

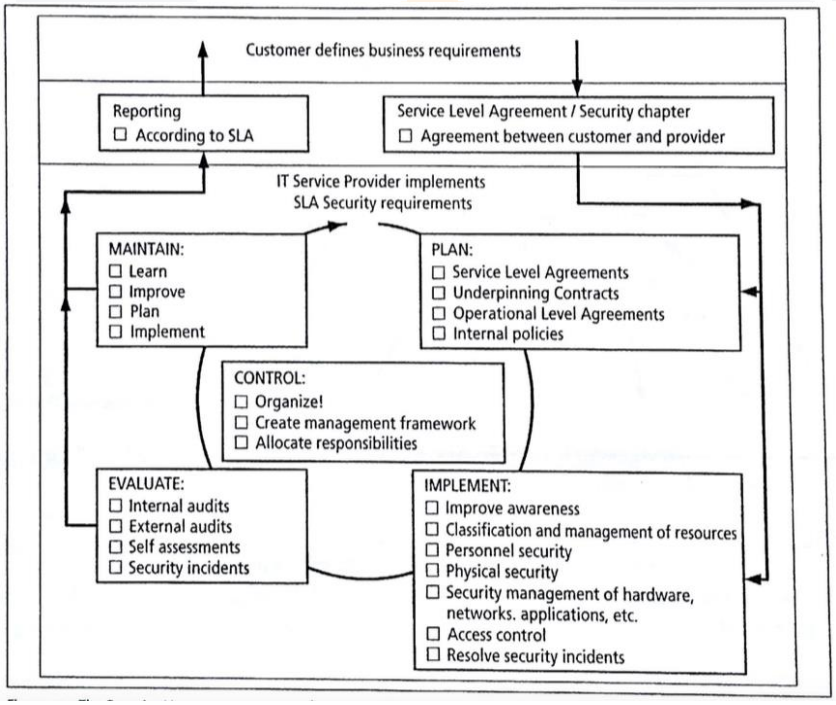


Figura 6 El proceso de gestión de la Seguridad (fuente ITSM Library)

Gestión de la seguridad tiene vínculos con otros procesos de ITIL.

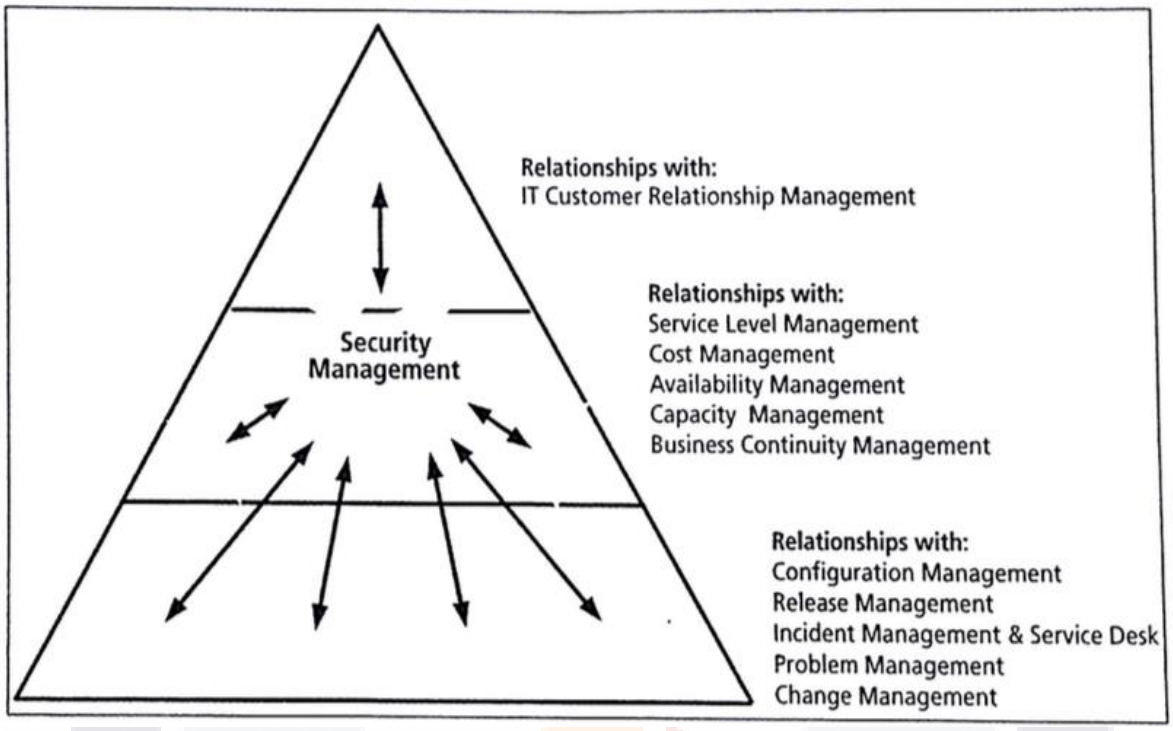


Figura 7 Gestión de la Seguridad de las relaciones con otros procesos

3.2.3 Actividades

1. Control : política de seguridad de la información y la organización

La actividad de control es el centro del subproceso de administración de seguridad y se refiere a la organización y gestión del proceso.

Esta actividad define los subprocesos, las funciones de seguridad, los roles, las responsabilidades y también se describe a la estructura organizativa, los mecanismos de rendición de informes y en la línea de control (que indica a quién, quién hace qué, ¿cómo está el tema de la aplicación?). Las siguientes medidas en el Código de Práctica se aplican en esta actividad:

- **Política:**
  - Desarrollo y aplicación de políticas.
  - Objetivos, principios generales y significado.
  - Asignar funciones y responsabilidades .
  - Los vínculos con otros procesos de ITIL y su gestión.
  - Tratamiento de incidentes de seguridad.

- **Organización de Seguridad de la Información:**
  - Estructura de gestión (estructura organizativa).
  - Asignación de responsabilidades con mayor detalle.
  - Establecer un comité directivo de seguridad de la Información.
  - Coordinación de Seguridad de la Información.
  - Acordar herramientas (p. ej. para el análisis de riesgos y mejorar la conciencia).
  - Descripción de las instalaciones de TI y su proceso de autorización.
  - Asesoramiento especializado.
  - Cooperación entre las organizaciones.
  - Las comunicaciones internas y externas. Auditoría de Sistemas de información independientes.
  - Principios de seguridad de acceso para terceros.
  - Seguridad de la información en los contratos con terceros.

2. Plan :

La planificación del proceso incluye la definición de la sección de seguridad relacionado con SLA (Service Level Agreement, acuerdo de nivel de servicio). Debe ser considerado de igual manera el plan de seguridad de nuestro proveedor de servicios y como un plan de seguridad específico, por ejemplo, para cada plataforma, aplicación o red en la organización, se planean las políticas de seguridad para la organización, logrando definirlas.

3. Implementación

La aplicación subproceso tiene por objeto poner en marcha todas las medidas especificadas en los planes. La siguiente lista de comprobación puede apoyar este subproceso.

- Clasificación y manejo de los recursos de TI (acorde a las directrices)
- Seguridad del Personal:
  - Descripciones de puestos de trabajo.
  - Acuerdos de confidencialidad para el personal.
  - Directrices para el personal para tratar con incidentes de seguridad y observar las debilidades de seguridad.
  - Las medidas disciplinarias.
  - Conciencia de la seguridad
- Gestión de la seguridad:
  - Cumplimiento de las responsabilidades.
  - Instrucciones de funcionamiento (por escrito).
  - Reglamentos internos.
  - Cubrir el desarrollo de sistemas, pruebas, aceptación, operaciones, mantenimiento y eliminación.
  - Separación de los entornos de desarrollo y pruebas del entorno de producción.
  - Los procedimientos para tratar los incidentes (Gestión de incidencias).
  - La aportación a la gestión del cambio.
  - Aplicación de medidas de protección antivirus.
  - Aplicación de medidas de gestión de equipos, aplicaciones y redes.
  - Manejo y seguridad de los datos en los medios de comunicación.
- Control de acceso:
  - Normas de control de acceso (programa).

- Mantenimiento de los privilegios de acceso.
- Mantenimiento de la seguridad en la red.
- Aplicaciones para identificación y autenticación.

4. Evaluar

Una evaluación independiente de las medidas previstas es esencial. Esta es necesaria para evaluar el rendimiento y también es requerido por los clientes y terceros, se pueden usar para actualizar las medidas acordadas, en sugerir cambios, en cuyo caso se presentó al proceso de Gestión de cambios.

Hay tres formas de evaluación:

- Auto- evaluaciones.
- Las auditorías internas.
- Las auditorías externas.

También se realizan evaluaciones en respuesta a incidentes de seguridad.
Las actividades principales son:

- Verificar el cumplimiento de las políticas y la aplicación de medidas de seguridad.
- Realizar auditorías de seguridad en los sistemas de información.
- Identificar y responder a la utilización inapropiada de los recursos de TI.

5. Mantenimiento

La seguridad requiere mantenimiento, como el riesgo del cambio debido a los cambios en la infraestructura, la organización y los procesos de negocio. Mantenimiento de la seguridad incluye el mantenimiento de la sección de seguridad del SLA y el mantenimiento de los planes detallados. Mantenimiento se lleva a cabo sobre la base de los resultados de la evaluación.

6. Informes

La presentación de la información no es un subproceso , es una salida de los otros subprocesos. Los informes se preparan para proporcionar información sobre el rendimiento de seguridad y para informar a los clientes sobre cuestiones de seguridad. Estos informes son generalmente necesarios en virtud de un acuerdo con el cliente. La información es importante, tanto para el cliente como para el proveedor del servicio. Los clientes deben estar correctamente informados sobre la eficacia de los esfuerzos (por ejemplo, con respecto a la aplicación de las medidas de seguridad) y las medidas de seguridad concretas. Para informe sobre incidentes de seguridad definidos en el SLA, el servicio debe tener un canal directo de comunicación con un representante del servicio al cliente.

3.3 Procesos Relacionados a Gestión de Seguridad (Security Managment) en MOF v3

Microsoft® Operations Framework (MOF) proporciona orientación operativa que permite a las organizaciones lograr confiabilidad en misiones críticas del sistema, disponibilidad, compatibilidad y capacidad de gestionar productos y tecnologías. MOF tiene como base ayudar a la mejora continua de los servicios de TI de una forma más procesable y alcanzable, se basa en la mejor orientación práctica contenida en la versión MOF 3 y se posiciona para la compatibilidad con futuras versiones de MOF y la Biblioteca de Infraestructura de TI (ITIL).

MOF esta constituido por tres componentes:

- Evaluación de Gestión de Servicios
- Programa de Mejoramiento de Servicio
- Guia de Orientación de Servicios

Donde Guia de Orientación de Servicios consta de cuatro cuadrantes :

- El Cuadrante de Optimización

Las organizaciones deben alinear sus servicios de TI con sus procesos de negocio. Para ellos, las prácticas de optimización que se encuentran en MOF ayudan a guiar una gestión más eficaz en el nivel de servicio, planificación de la capacidad y otros esfuerzos de planificación de largo alcance.

- El Cuadrante de Cambio

A través de MOF, se pueden mejorar los procesos de gestión de servicios de TI en todas las etapas de su ciclo de vida.

- El Cuadrante de Soporte

MOF en este cuadrante describe procesos y prácticas necesarias para apoyar plenamente el uso eficiente de una infraestructura de TI.

- El Cuadrante de Operación

La mejora de la eficiencia operativa puede mejorar en gran medida el valor de las TI para el negocio.

3.3.1 Gestión de Seguridad

Gestión de seguridad en MOF versión 3 se encuentra en el cuadrante de Optimización, donde describe los procesos esenciales y las actividades que se requieren para establecer y mantener un buen programa de seguridad para toda la organización.

Los beneficios resultantes son:

- El adecuado nivel de seguridad, confidencialidad, integridad y disponibilidad de información para cada activo basándose en su valor en el negocio, su susceptibilidad a una infracción de la seguridad y el coste de la aplicación de la protección necesaria.
- Minimiza las interrupciones en el funcionamiento de la empresa que son resultados de los incidentes de seguridad.
- Adapta continuamente políticas y procedimientos de seguridad, los cuales se adaptan a los cambios en la organización objetivos de la empresa, el entorno externo, las amenazas a la seguridad, la aparición y el uso de nuevas tecnologías.

3.3.2 Descripción general del Proceso de Gestión de Seguridad

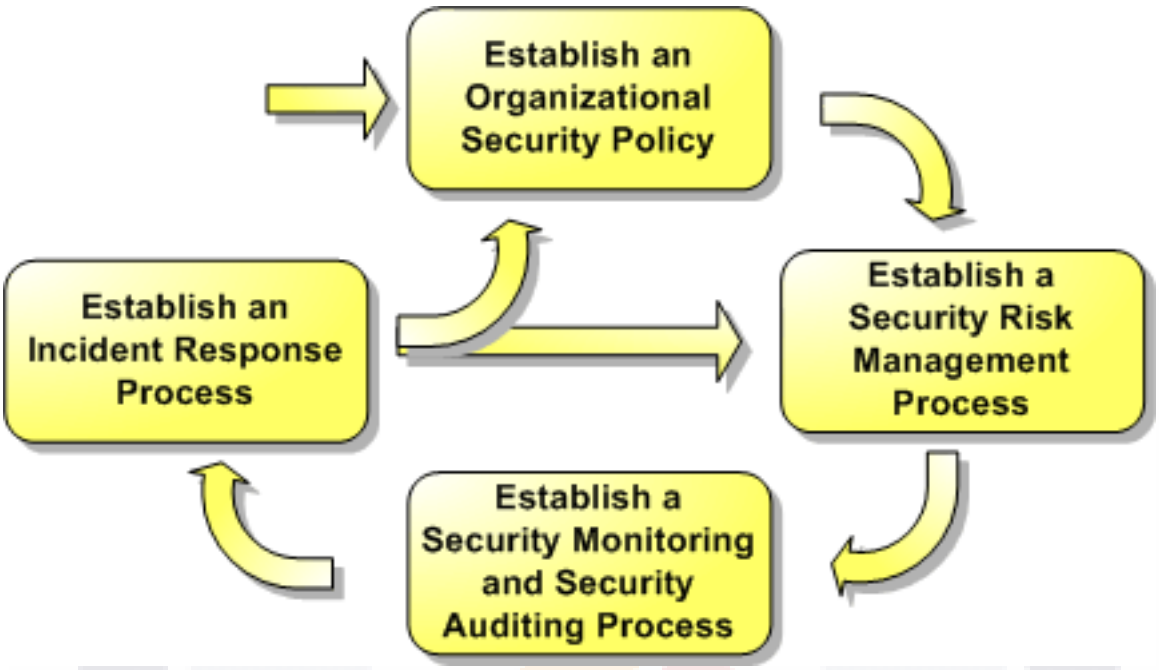


Figura 8 Relación entre los procesos de Gestión de Seguridad (MOF v3)

Establecer una política de seguridad organizacional

Para desarrollar un programa de seguridad, es necesario reunir un equipo de actores clave para impulsar la iniciativa. El equipo, llamado el Comité Directivo de Seguridad, es el responsable de la toma de decisiones antes y después de la aplicación de los programas de seguridad.

- Visión y Misión (Seguridad)
- Las entradas para la planificación de políticas
- Clasificación de datos (confidencial, privado, Sensibles, público)
- Planificación de Políticas

Planificación generalmente comienza a crear un esquema que muestra los objetivos organizacionales para la política. Una política también sirve como una referencia. Por esta razón, una política de seguridad debe incluir una tabla de contenido, un glosario y un índice.

Figura 9 Jerarquía política de seguridad (MOF v3)

- Roles y Responsabilidades

El desarrollo y la aplicación de una organización requiere un programa de seguridad personal modelo que puede apoyar los objetivos del programa. Esto no significa que la organización debe reestructurar, dado que en las funciones que ya existen otras responsabilidades.

Cuando se selecciona personal de seguridad, escoger a la gente que puede aportar un nivel de sus conocimientos en materia de seguridad de información.

En las dos tablas siguientes se identifican las funciones individuales y de grupo, así como sus responsabilidades según MOF.

Tabla 1 Funciones y responsabilidades individuales (MOF v3)

Las funciones individuales	Responsabilidades
Director	Actuar como promotor para el desarrollo de la política de seguridad organizativa. Un ejecutivo, tales como el jefe de seguridad o jefe de información, llena este papel. Esta función sirve también como el último punto de extensión para definir riesgo aceptable para el negocio.
Administrador de seguridad	Liderar el desarrollo de la organización y las políticas relacionadas con la seguridad. Toda la responsabilidad de la elaboración de políticas, la toma de conciencia y la clasificación de datos.
Gestor de operaciones	Apoyar iniciativas en materia de seguridad, asignar y dirigir los recursos para realizar los objetivos de seguridad de la organización.
Gestor de negocios	Apoyar el desarrollo de una política de seguridad que ofrece un beneficio empresarial, proporcionando un punto de vista comercial para una persona departamento o división.
Arquitecto de seguridad o profesional de la seguridad	Proporcionar conocimientos de seguridad, especialista en los procesos de diseño, planificación, implementación, mantenimiento y auditarías de las políticas de seguridad de la empresa.
Datos o propietario del servicio	Ser responsable de datos específicos o servicio activo en la organización. La responsabilidad de mitigar los riesgos de estos activos.
Administrador de datos o Custodio de datos	Tienen la responsabilidad administrativa en el día a día de gestionar la seguridad de los activos.
Administrador de seguridad	Definir y aplicar las políticas de seguridad. Gestionar la seguridad de los accesos a los activos de la organización. Control de seguridad y supervisar los procesos que mantienen un entorno informático seguro.
Auditor	Ayuda interna o externa independiente a la auditoría de seguridad para comprobar que las políticas de seguridad y los

Las funciones individuales	Responsabilidades
	controles de la organización están operando de manera efectiva.
Usuario	Apoyo y seguimiento a las orientaciones de las políticas de seguridad en el manejo de los recursos de la información.

Tabla 2 Roles y Responsabilidades (MOF v3)

Roles del grupo	Responsabilidades
Grupo de seguridad de la información	Desarrollar las políticas de seguridad de todos los activos de la organización y proporcionar mayor seguridad de la información. Definir los requisitos de seguridad funcional y medir el control de la eficacia general del programa de seguridad, sobre la base de insumos internos y externos. Crear contenido de programas de sensibilización. Este grupo tiene funciones permanentes. Los miembros pueden incluir las siguientes funciones: • Administrador de seguridad • Gestor de operaciones • Gestor de negocios
Comité directivo de seguridad	Establecer y conducir a la adopción del programa de seguridad en una perspectiva comercial y de negocios. Respecto a la seguridad de la organización, la visión y los objetivos de todo el personal. Aprobar la asignación de recursos suficientes para el programa. Asegúrese de que se asignen las responsabilidades. Vigilar el progreso global del programa. Este grupo está involucrado principalmente en la planificación, el diseño y las primeras etapas de aplicación. Los Miembros pueden incluir las siguientes funciones: • Director

Roles del grupo	Responsabilidades
	• Administrador de seguridad □ • Gestor de operaciones • Gestores de negocios
Equipo Administración de Riesgos de seguridad	De la empresa y equipo de negocios, personal de seguridad que se encarga de conducir el proceso de administración de riesgos de seguridad. Este proceso mantiene el riesgo de seguridad dentro de la organización a un nivel aceptable. Este grupo tiene las funciones permanentes. Los miembros pueden incluir las siguientes funciones, o sus funcionarios encargados de ella: • Administrador de seguridad • Gestor de operaciones□ • Gestores de negocios
Equipo de respuesta a Incidentes de seguridad	Gestión de incidentes de seguridad escalada. Este equipo debe tener miembros con buen conocimiento de las amenazas a la seguridad, tales como: • Las operaciones de la empresa • Las funciones de TI • Los procedimientos de escalabilidad • Planificación de Contingencia Este grupo tiene funciones permanentes. Los miembros pueden incluir las siguientes funciones: • Administrador de seguridad • Gestor de operaciones • Auditor
Grupo de Tecnología de la información	Este grupo incluye la arquitectura, la ingeniería, auditoría y las operaciones.

- Conciencia

La política no es de uso si las personas de una organización no están familiarizados con el contenido de la misma. También es importante que el personal comprenda la forma en que las políticas afectan a ellos y a sus puestos de trabajo. Crear un programa de concienciación en seguridad para que el sistema mantenga actualizados a los usuarios de los cambios y las nuevas políticas es otro aspecto de un exitoso programa de seguridad.

Establecer un proceso de administración de riesgos de seguridad

El proceso de administración de riesgos de seguridad produce un entorno de control eficaz que se ha diseñado para minimizar el riesgo empresarial a un nivel aceptable. El nivel de riesgo aceptable varía entre las organizaciones.

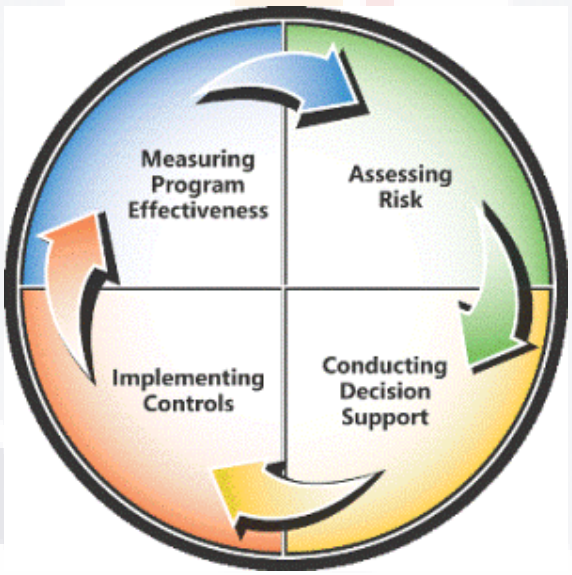


Figura 10 Las fases del proceso de administración de riesgos de seguridad (MOF v3)

- Evaluación de Riesgos

Los objetivos de la evaluación del riesgo son: identificar y priorizar los riesgos en toda la organización. El primer paso en la evaluación del riesgo fase es la planificación, después de la planificación, el siguiente paso es identificar el

riesgo de otorgar información relacionada con los grupos interesados en toda la organización, el último paso en la evaluación de riesgo es la fase de prioridades.

- Realizar Soporte de decisiones

El objetivo del soporte de decisiones es seleccionar los controles de seguridad adecuados para aplicar dentro de la organización. Para ello, el apoyo a la toma de decisiones utiliza la lista de prioridades de los riesgos definidos durante la evaluación del riesgo y se centra en el más alto riesgo identificado.

- Implementación de controles

El objetivo de la de implementación de controles es garantizar la priorización de las soluciones de control, para que las partes interesadas estén acordes durante el proceso de apoyo a las decisiones, e implementarlas correctamente. Este proceso implica desarrollar planes de acción para implementar los controles en un período de tiempo específico con interrupciones mínimas para el negocio.

- Medición de la eficacia del programa

El objetivo de la medición de la eficacia del programa es determinar cómo el control frente a los riesgos está en evolución. Idealmente, los resultados obtenidos confirman el progreso de la organización hacia su objetivo de reducir los riesgos a niveles aceptables.

Establecer un control de seguridad y un proceso de auditoría de seguridad

Control de la seguridad y auditoría de seguridad comprende dos actividades principales.

- Supervisión de la seguridad

Los administradores de seguridad se preocupan por los eventos del sistema atípicos. El objetivo general es proteger los sistemas y la seguridad de los datos que contienen. Examinar los registros detallados de las operaciones de un sistema ayuda a realizar esta tarea.

El proceso de administración de riesgos de seguridad ayuda a las organizaciones a evaluar sus activos, determinar qué controles son necesarios y el nivel de supervisión que se requiere. También es importante para determinar la diferencia entre las condiciones típicas y atípicas e identificar las medidas apropiadas para llevar a cabo cuando existan condiciones atípicas.

Figura 11 Análisis de incidentes y eventos recomendaciones (MOF v3)

- Auditoría de seguridad

La auditoría de seguridad, también se conoce como el cumplimiento de la política de seguridad, es responsabilidad del Grupo de Seguridad de la Información, este grupo:

- Utiliza las herramientas y técnicas para detectar e informar sobre los elementos dentro del sistema que no cumplan con la política de seguridad de la organización de manera proactiva.

- Confirma si los sistemas están configurados correctamente, si los usuarios están funcionando correctamente y si los datos están protegidos.
- Asegura que los controles de seguridad están configurados y funcionando correctamente.

Cualquier artículo, u otras vulnerabilidades que no son compatibles, se investigan, la causa determinada y las medidas correctivas puestas en su lugar. Esto puede implicar la formación de los empleados, la clarificación de controles específicos y procedimientos relacionados, o incluso la modificación de las políticas de seguridad.

Establecer un Proceso de Respuesta a Incidentes

El proceso de respuesta a incidentes define la forma en que los incidentes de seguridad se informan y se proporcionan respuestas apropiadas. Los incidentes van desde los que son solamente registrados a los que se requiere una acción inmediata, de toda la organización para mitigar los efectos de un fallo de seguridad.

Los objetivos del proceso de respuesta a incidentes son:

- Desarrollar las reacciones efectivas y oportunas a los incidentes de seguridad.
- Asegurar que un incidente de seguridad no pueda volver a ocurrir.

- Responsabilidades de Información del usuario:

Muchos tipos de incidentes de seguridad son indetectables mediante controles técnicos, o no es rentable hacerlo. Por ejemplo, los usuarios que no pueden bloquear sus ordenadores cuando salen de sus escritorios, esto puede significar incidentes de seguridad de información.

- La escolarización del Equipo a Respuestas de Incidentes:

Independientemente del tipo de incidente, el proceso de respuesta para hacer frente a cualquier incidente de seguridad debe ser coherente, bien documentado y acordado por todas las partes pertinentes de TI. Este equipo debe emplear su experiencia así como asegurar que es una vía de escalamiento y poder manejar cualquier situación, sin importar cuán serio es el incidente de seguridad.

- Evaluación de Incidentes:

Es importante para capturar información de incidentes de seguridad contar con la mayor precisión y lo mas detallada como sea posible. Teniendo en cuenta el comprender para lo que esta información será utilizada, no sólo operacionalmente sino también estratégicamente.

3.4 Procesos Relacionados a Gestión de Seguridad (Information security management) en ISO/IEC 20000

ISO/IEC 20000 normalizado y publicado por las organizaciones ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission) el 14 de diciembre de 2005, es el estándar reconocido internacionalmente en gestión de servicios de TI.

El tema de Gestión de Seguridad es tratado en el sexto capitulo de la norma con el nombre Procesos de prestación de servicio donde sus subcapítulos son :

Gestión de seguridad de la información
- Política de seguridad de la información
- Controles de seguridad de la información
- Cambios de seguridad de información e incidentes

El objetivo de la gestión de seguridad de la información es ser efectiva en todas las actividades de servicio.

Una gestión con autoridad competente aprobará una política de seguridad de la información que deberá ser comunicada a todo el personal pertinente y clientes cuando proceda.

Los controles de seguridad adecuados se aplicarán a:

a) Los requisitos de la política de seguridad de la información.
b) Gestionar los riesgos asociados con el acceso a los servicios o sistemas.

Los controles de seguridad deberá estar debidamente documentados. La documentación deberá describir los riesgos a los que los controles se refieren, a la manera de operación y al mantenimiento de los controles.

Acuerdos que impliquen la presencia de las organizaciones que tengan acceso a los sistemas y servicios de información se basarán en un acuerdo formal en el que define los requisitos de seguridad necesarios.

Incidentes de seguridad deberán ser reportados y registrados de conformidad con la gestión de incidencias del procedimiento tan pronto como sea posible. Se adoptarán los procedimientos para asegurar que todos los incidentes de seguridad sean investigados y tomar las medidas de gestión adoptadas.

Seguridad de la Información es el resultado de un sistema de políticas y procedimientos diseñados para identificar, controlar y proteger la información y los materiales utilizados en relación con el almacenamiento, la transmisión y el procesamiento.

El proveedor de servicios de personal con información especializada las funciones de seguridad debe estar familiarizado con la norma ISO/IEC 17799. Tecnología de la Información - técnicas de seguridad - Código de buenas prácticas de gestión de la seguridad de la información.

Identificar y clasificar los activos de información

El proveedor de servicio debe:

a) Mantener un inventario de los activos de información (por ejemplo, computadoras, comunicaciones, equipos para la protección del medio ambiente, documentos y otra información) que son necesarias para la prestación de servicios.
b) Clasificar cada uno de los activos de acuerdo con su importancia para el servicio y el nivel de protección que requiere y nombrar a un propietario a ser el responsables de proporcionar esa protección.
c) La obligación de rendir cuentas para la protección de activos debería estar en manos de los propietarios de activos, aunque pueden delegar día a día responsabilidades de gestión de la seguridad.

Las prácticas de evaluación de riesgos de seguridad

Evaluación de riesgos de seguridad debe:

a) Realizarse en intervalos especificados.
b) Estar registrados.
c) Mantenerse durante los cambios de las necesidades cambiantes de la empresa, procesos y configuraciones.
d) Ayudar para la comprensión de lo que podría tener un impacto un servicio gestionado.
e) Tomar decisiones con respecto a los tipos de controles.

Riesgos a los activos de información

Los riesgos de los activos de la información deberían ser evaluados en relación a:

a) Su naturaleza (p.ej. fallo de software, errores de operación, fallos de comunicaciones)
b) Probabilidad
c) Posible impacto en las empresas
d) Experiencia adquirida en el pasado

Seguridad y disponibilidad de la información

En la evaluación de los riesgos se debe tener en cuenta lo siguiente:

a) Divulgación de información confidencial a partes no autorizadas.
b) Posible información inexacta, incompleta o no válida.
c) Información que no esté disponible para su uso.
d) Daños físicos o la destrucción de equipos necesarios para la prestación de servicios.

También se debe tener en cuenta de la seguridad de la información los objetivos, políticas, la necesidad de satisfacer sus requisitos de seguridad especificados y requisitos legales o reglamentarios que se aplican.

Controles

Además de otros controles que pueden estar justificados y asesorados en otras partes de la norma ISO/lec 20000 (p. ej., en continuidad del servicio), los proveedores de servicios deben operar los siguientes controles en áreas de una buena gestión de la seguridad de la información práctica.

a) Los directivos deben definir sus políticas de seguridad de la información, que comunicarán al personal, a los clientes y actuar para garantizar su aplicación efectiva.
b) Gestión de la seguridad de la información, funciones y responsabilidades deben ser definidas y asignadas a los titulares.
c) Un representante del grupo de gestión debe vigilar y mantener la eficacia de la Política de Seguridad.
d) Personal con importantes funciones de seguridad de la información deben recibir capacitación.
e) Todos los funcionarios deben ser conscientes de la política de seguridad de la información.
f) Ayuda de expertos en la evaluación de riesgos y control de la ejecución deben estar disponibles.
g) Los cambios no deben comprometer el funcionamiento eficaz de los controles.
h) La información de incidentes de seguridad debería ser informada al los procedimientos de gestión de incidencias y la respuesta.

Los documentos y registros

Los registros deben ser analizados periódicamente para proporcionar a la dirección información sobre:

a) Eficacia de política de seguridad de la información.
b) Las nuevas tendencias en la seguridad de la información de incidentes.
c) Entrada a un plan de mejoramiento del servicio.
d) Control de acceso a la información, bienes y sistemas.

El sistema de gestión de seguridad de la información debe ser documentado.

3.5 Análisis y descripción de procesos de IDEF0

IDEF0 o IDEFØ (por sus siglas en ingles Integration Definition for Function Modeling) método derivado de SADT (Structured Analysis and Design Technique), la Fuerza Aérea de los Estados Unidos desarrollo el método de modelado para analizar y comunicar los procesos de un sistema.

Un modelo efectivo de IDEFØ ayuda a organizar el análisis de un sistema y a promover una buena comunicación entre el analista y el cliente. IDEFØ es útil para lograr establecer el alcance de un análisis. Como herramienta de comunicación, IDEFØ mejora la participación de expertos de dominio y consenso en la toma de decisiones a través de dispositivos gráficos simplificados.

- Simbología

Figura 12 Simbología de IDEF0

Los elementos se describen a continuación:

1. Función o Actividad: Frase verbal (Verbo + objeto directo), es representada por una caja. Indica la función que será modelada y

proporciona una descripción de lo que pasa en ella. La caja debe tener un nombre que describa la función.

2. Entrada(s): representadas por una flecha de flujo entrante del lado izquierdo de la caja de una actividad o proceso. Indica el material o información consumida o transformada por una actividad para producir salidas.
3. Salida(s): representadas por flechas de flujo saliente del lado derecho de la caja de una actividad o proceso. Son los datos u objetos producidos por la actividad o proceso y pueden ser transmitidos a otras actividades o procesos.
4. Control(es): representadas por flechas de flujo entrante en la parte superior de la caja de una actividad o proceso. Especifican las condiciones requeridas por la actividad para producir salidas correctas. Por ejemplo: Normas, guías, políticas, especificaciones, procedimientos, etc.
5. Mecanismos: representados por flechas de flujo entrante en la parte inferior de la caja de una actividad o proceso. Indican los medios o recursos que brindan soporte para la ejecución de la actividad. Por ejemplo: Maquinas, programas de cómputo, instalaciones, recursos humanos, sistemas de información, etc.
6. ID: Identificador para cada actividad.
7. En la parte inferior del diagrama se incluirán 3 datos: El nivel del diagrama (A0), la Organización y entre paréntesis el nivel ejemplo: "LabDC-UAA (Nivel General)" y finalmente el número de hoja que en éste caso siempre es 1.

- Reglas

1.- A partir del nivel A0 el más generalizado, los niveles inferiores van detallando más los procesos.

Para el modelado a nivel intermedio primeramente se utilizará el nivel A1. Al detallar los diagramas hijos se utilizará la siguiente jerarquía: por ejemplo si se desea modelar el siguiente nivel del proceso 2 del modelo A2 el diagrama resultante será el A22. Otro ejemplo, si se desea modelar el siguiente nivel del proceso del modelo A3 el diagrama resultante será el A23 como se muestra en la figura:

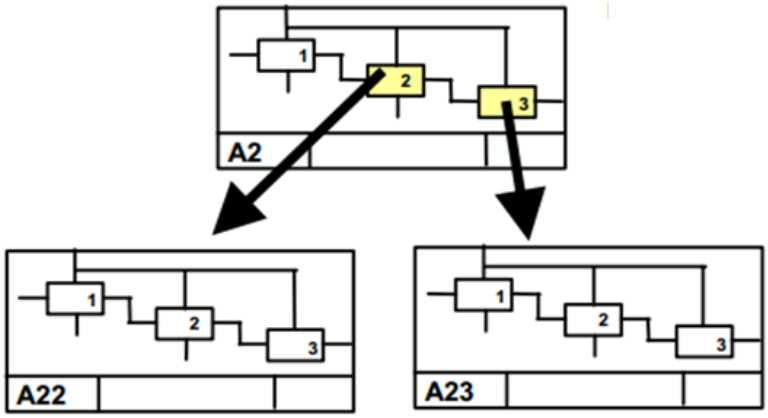


Figura 13 Casos jerarquías

2.- En cada diagrama hijo (por ejemplo el diagrama A1 es hijo del diagrama A0) se representarán todas las entradas, mecanismos, controles y deberá arrojar las mismas salidas. Como se muestra en la siguiente figura.

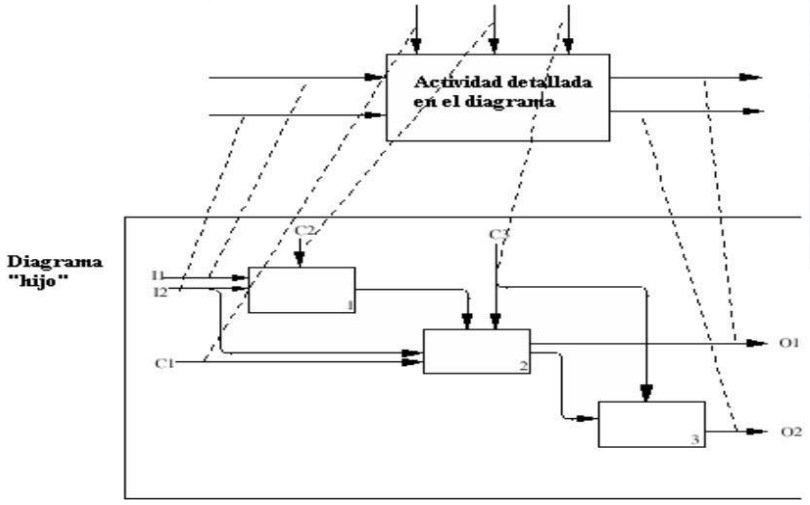


Figura 14 Diagrama hijo entradas y salidas

Será posible realizar interconexiones entre las entradas, salidas, mecanismos y controles como se explica en las siguientes reglas:

3.- La salida de una actividad puede ser la entrada de otra.

4.- La salida de una actividad puede ser el control de otra.

5.- La salida de una actividad puede ser el mecanismo de otra actividad.

6.- La salida de una actividad puede ser el control a modo de retroalimentación de otra actividad anterior.

7.- La salida de una actividad puede ser una entrada a modo de retroalimentación de otra actividad anterior.

3.6 Revisión de Casos Similares

3.6.1 Ejemplo 1 : Estandarización de Seguridad en TI (IT security standardisation, 2004, Dr Walter Fumy)

Algunos sistemas de cortafuegos e IDS (Intrusion Detection System) tienen la capacidad de realizar un análisis de nivel de aplicación. Por ejemplo IDS se puede configurar para buscar cadenas específicas en un URL. Palabras clave, las cuales pueden ayudar a localizar a los usuarios que violen la política interna y potencialmente violan la ley. Y una regla de firewall que registra todo el acceso a Gmail, Hotmail y otros servicios de correo gratuitos se pueden detectar rápidamente a los usuarios que acceden a correo electrónico personal en horas de trabajo, el mal uso de Email viene en muchas formas, como para el robo de información de la empresa.

" Es inevitablemente, el establecimiento de normas de seguridad de tecnología de la información significa ponerse al día con la tecnología y el ingenio de las personas que atacan a los sistemas de TI. Pero hay que hacerlo"(Dr. Warnel Fumy).

Hay un creciente reconocimiento de la necesidad de una amplia gama de normas de seguridad informática y directrices técnicas para apoyar la seguridad cibernética, tanto a nivel nacional como internacional. Tanto los gobiernos como el sector privado tienen un papel importante que desempeñar en el desarrollo, implementación y promoción de dichas normas.

Sistemas, redes y políticas deben ser diseñadas adecuadamente, aplicarse y conseguir optimizar la seguridad. La especificación y adopción de soluciones (tanto técnicos como no técnicos) apropiadas para evitar o limitar el daño potencial de las amenazas y vulnerabilidades identificadas. Afortunadamente, un número de estándares están disponibles o en desarrollo.

También hay una continua necesidad de revisar las políticas, medidas y procedimientos para asegurar que cumplan con los cambiantes desafíos que plantean las amenazas a los sistemas de TI y redes.

Los expertos coinciden en que el principal desafío para las empresas y el sector público de hoy no es la tecnología de seguridad en sí, sino la forma de establecer los procedimientos adecuados, la gestión y los controles para el logro de la seguridad informática. Los seres humanos seguirán siendo menos fiables y menos fáciles de predecir que las tecnologías de seguridad. La formación y la educación, así como el apoyo y compromiso de la alta dirección continuarán siendo cuestiones clave entorno al tema de seguridad informática.

3.6.2 Ejemplo 2 : La implementación de seguridad en la empresa: un caso de estudio (Implementing enterprise security: a case study, 2003, Ken Doughty)

La información es un activo esencial para las organizaciones, ya que apoya las operaciones del día a día y facilita la toma de decisiones de los actores clave de la organización. El desafío que enfrentan las organizaciones es cómo proporcionar acceso a este activo sin comprometer su integridad. Este activo es recibido y distribuido por la organización a través de diferentes canales de distribución, que se conectan entre sí por la red de las telecomunicaciones. Estos canales incluyen:

- Correo electrónico
- Internet
- Las aplicaciones (por ejemplo, Financiera, Logística, Inmobiliario y Construcción, Energía, etc.)
- DBMS (MS SQL Server, Oracle, DB2, Sybase, etc.)
- Los sistemas operativos (por ejemplo, Unix, NT / Windows 2000, etc.)

Aunque la piratería y los virus pueden ser considerados como la amenaza más inmediata y mayor a las organizaciones en la actualidad, existen riesgos de

seguridad en otras áreas que a menudo no son tratados adecuadamente. La educación del personal en el control de la empresa y la información confidencial es un buen ejemplo.

Encuestas indican una vez más que la seguridad no está todavía siendo tratada por las organizaciones como una inversión en la protección de sus activos de información.

En el caso de estudio se aplicaron diferentes estrategias:

Estrategia de Seguridad:
Se realizó un enfoque estratégico y táctico para abordar la seguridad de 'lock-down' el medio ambiente dentro de una corta línea de tiempo de seis meses, (según la directiva CEO).
Los recursos disponibles para ser desplegadas fueron construidos por asignación del presupuesto del año anterior, se requiere un enfoque rentable y de valor añadido. Se tuvo en cuenta la plena aplicación de la norma ISO 17799. Sin embargo, el costo estimado era prohibitivo y no pudo ser implementado dentro del plazo. Por lo tanto, la estrategia fue implementar los elementos críticos de la norma ISO 17799 y sin el inhibidor de costo y dentro de la línea de tiempo. La estrategia también debía tener en cuenta la necesidad de la prestación continuada del servicios de TI para el negocio. Gestión Ejecutiva aprobó la estrategia antes de su ejecución. Este apoyo fue fundamental para facilitar la aplicación y la propiedad futura de la seguridad.

Estrategia táctica:
Un Proyecto de Seguridad se estableció con un director de proyecto dedicado. La organización ya había implementado una metodología de gestión de proyectos corporativos que se basa en el Project Management Institute (www.pmi.org). Este fue el primer proyecto para utilizar la metodología de gestión de proyectos. Un plan táctico fue desarrollado para dividir la implementación de la seguridad en cinco fases, estas fases fueron:

1. Organización (es decir, Políticas y Procesos).
2. Sistema Operativo.
3. Sistemas de gestión de base de datos (DBMS).
4. Telecomunicaciones.
5. Acceso - Activos de Información.

El Auditor de TI realiza una función de control de calidad durante toda la vida del proyecto y proporciona una serie de recomendaciones que:

- Dirigen a una mejora en la calidad de la entrega.
- Minimicen la probabilidad de fallos de seguridad que no se tratan adecuadamente.

Conclusiones del Dr. Ken Doughty: la implementación de seguridad de la empresa es una tarea enorme, pero muy gratificante cuando todo se junta. El Proyecto de Seguridad fue entregado a tiempo y dentro del presupuesto. Esto sólo fue posible gracias a la dedicación del personal del departamento de TI y el apoyo continuo de TI Auditor de la organización durante la vida del proyecto.

3.6.3 Ejemplo 3 : Respuestas a incidentes de seguridad de información (Information security incident response, 2004, Dr Abiola Abimbola)

En este artículo se aborda la información de respuesta a incidentes de seguridad, un aspecto importante de la seguridad de la información que incluye técnicas de gestión y las cuestiones jurídicas. Para lograr lo anterior, se discuten los roles y responsabilidades, proceso de escalamiento, la comunicación, los roles de compromiso, los incidentes de seguridad de la información y asuntos legales relacionados.

Las organizaciones invierten en medidas preventivas de seguridad para proteger sus activos de una violación de la confidencialidad, la integridad y la pérdida de calidad de servicios de Seguridad por la prevención no es suficiente. Mecanismos de respuesta adecuados son necesarios cuando un incidente de

seguridad relacionado, donde denota que el tema aun esta bastante amplio para futuras investigaciones.

Un método de los incidentes de seguridad es que el personal deba adoptarse para acelerar la respuesta y mitigar los daños así como tener en cuenta también un plan de seguridad de que se debe hacer en caso de un incidente.

La metodología cuenta con los puntos :

- Roles y responsabilidades
  Es importante definir las funciones y responsabilidades del personal clave.
- Escalamiento
  Es importate que las personas adecuadas tomen las decisiones correctas en el momento indicado.
- Comunicación, la regla del compromiso
  Mantener al margen la comunicación corporativa en todas las etapas.
- Incidentes de seguridad de información
  Desplegarán varios controles técnicos para mitigar las amenazas de seguridad y respuesta a todos los incidentes asociados
- Posibles escenarios de incidentes de seguridad de la información
  Existen varios posibles escenarios de incidentes de seguridad de la información los cuales deben conocerse.
- Las posibles respuestas a incidentes de seguridad informática
  Las acciones de respuesta a incidentes varían tanto para el corto y largo plazo.
- Asuntos legales relacionados
  Las leyes y reglamentos de la empresa deben ser políticas claras.
- Directrices de seguimiento
  El número de personas a las que se da a conocer cualquier material confidencial debe ser limitada.
- Guías para la publicación

También es importante observar ciertas pautas para la publicación de información sobre los empleados.

3.6.4 Ejemplo 4 : La estandarización de la Gestión de Seguridad en incidentes: el enfoque de ITIL (Security standardization in incident management: the ITIL approach, 2007, Dario Forte)

Un hito de ITIL es el desarrollo de un modelo eficaz de gestión de incidentes. Asegura continuidad del servicio en relación con los cuatro elementos de la Tecnología de la Información de Gestión de Servicios de TI (ITSM): organización, personal, tecnologías y procesos.

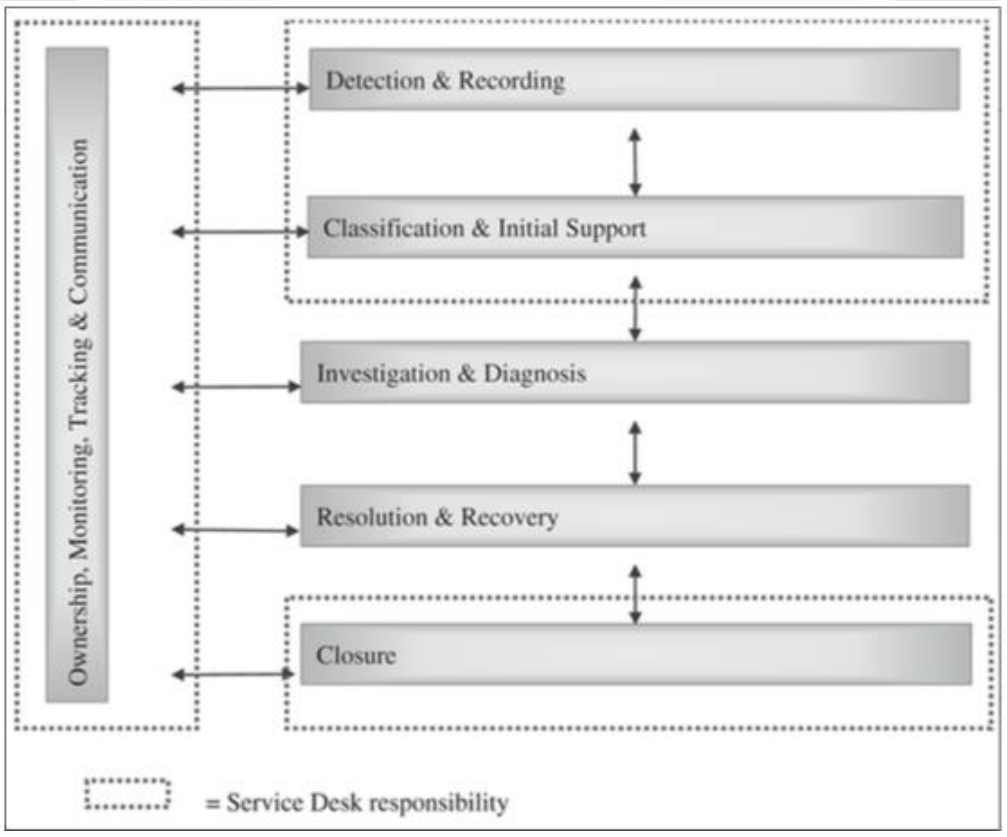


Figura 15 Componentes de proceso en ITIL modelo de gestión de incidentes

De acuerdo con las definiciones de ITIL más recientes, el objetivo principal de la gestión de incidentes es reducir al mínimo las interrupciones en las actividades empresariales y garantizar la disponibilidad del servicio.

La experiencia en el campo sugiere que el enfoque de ITIL para la gestión de incidentes es exactamente lo que pretende ser: un apoyo a la prestación de servicios. Pero si nos fijamos en lo estrictamente desde el punto de vista de seguridad nos vemos obligados a considerar que es insuficiente en términos de coherencia y eficacia.

No obstante, es posible tomar los componentes del proceso de ITIL y utilizarlos para mejorar la gestión de incidentes de seguridad. Pero esta no es la principal preocupación.

3.7 Contribuciones y limitaciones de teoría base y estudios similares.

De acuerdo a la literatura revisada sería de gran utilidad diseñar el proceso de gestión de seguridad de TI complementando el marco de ISO/IEC 20000 con ITIL v2 y MOF v3, debido a que es un proceso muy importante para garantizar una mejor calidad en los servicios y las propuestas actuales son de alto costo y alta complejidad para ser transferidas tal como son en organizaciones PYMES. Por ello, la necesidad de generar un proceso básico.

De la revisión a profundidad del marco teórico, se confirma la relevancia de usar estos marcos de gestión de TI y la carencia de uno para organizaciones PYMES. Así mismo se estudian herramientas de software que pudieran brindar soporte en dicho proceso, se han localizado algunas herramientas open source de las cuales se seleccionará la que mejor se adapte a las necesidades del caso de estudio (LABDC-UAA).

De igual manera se revisó una herramienta de modelado de funciones, a fin de poder emplearla para el modelado del proceso. Dicha herramienta es IDEF0, la cual permite modelar sistemas complejos presentándolos de manera comprensible.

Del estudio de los estándares ISO 20000, ITIL v2, Mof v3 se obtuvo una tabla comparativa entre las aportaciones de cada uno de los estándares al proceso de Gestión de Seguridad.

Tabla 3 Aportaciones al Proceso de Gestión de Seguridad de ISO 20000, ITIL v2 e ITIL v3

ISO 20000	MOF 3	ITIL v2
Identificar y clasificar los activos de información • Inventario de los activos • Clasificación de activos	Establecer una política de seguridad organizacional • Visión y misión • Las entradas para las políticas • Clasificación de datos	Control • Políticas • Seguridad de la información organizacional Plan

Evaluación de riesgos de seguridad, prácticas de seguridad y evaluación de riesgos • En periodos • Deben estar registrados Riesgos a los activos de información • Los activos deberán ser evaluados según su riesgo. Seguridad y disponibilidad de la información • Para la evaluación se debe analizar los posibles riesgos Controles • Definir políticas • Definir responsables de seguridad • Mantener la eficiencia de las políticas • Capacitación • Hacer conciencia de de las políticas • Expertos en riesgos y control • Cambios • Informes sobre incidentes Los documentos y registros • Se deben tener documentados	• Planificación de políticas • Roles y responsabilidades • Conciencia Establecer un Proceso de administración de riesgos de seguridad • Evaluación de riesgos • Realizar soporte de decisiones • Implementación de controles • Medición de la eficacia del programa Establecer un control de la seguridad y auditoría de seguridad Proceso • Supervisión de la seguridad • Auditoria de seguridad Establecer un Proceso de Respuesta a Incidentes • Responsabilidades de información del usuario	• Plan de seguridad específico Implementación • Clasificación y manejo de recursos • Seguridad del personal • Gestión de la seguridad • Control de acceso Evaluación • Auto-evaluaciones • Evaluaciones internas • Evaluaciones externas Mantenimiento • Riesgos de cambios • Aprender • Implementar Informes • Realizar informes

Procesos de gestión de la seguridad modelados con IDEF0:

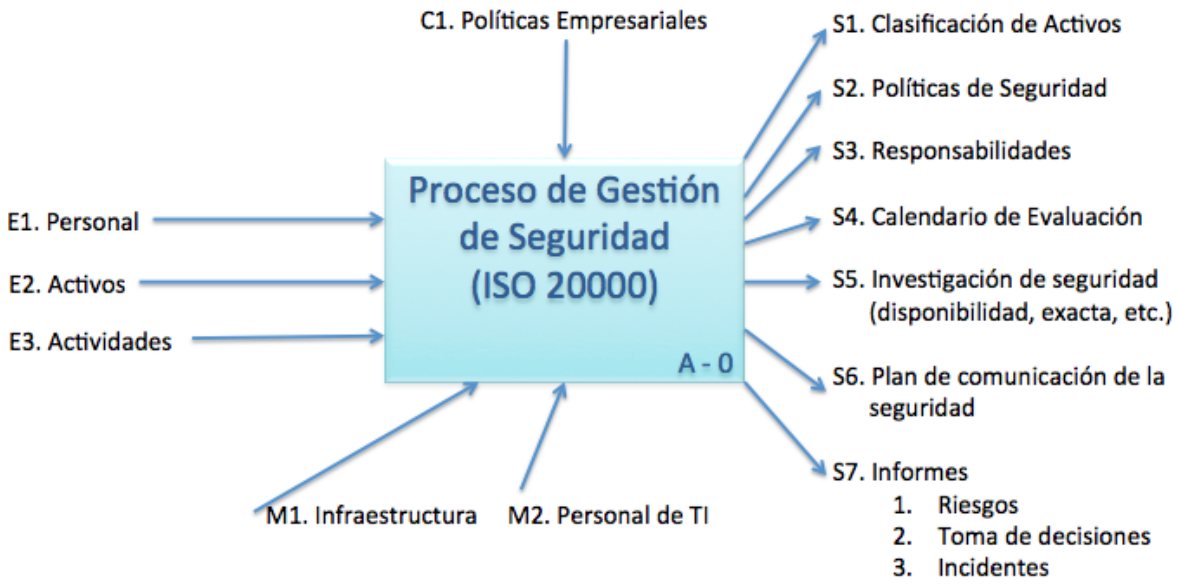


Figura 16 Proceso de Gestión de la Seguridad basado en ISO 20000

Figura 17 Proceso de Gestión de la Seguridad basado en ITIL v2

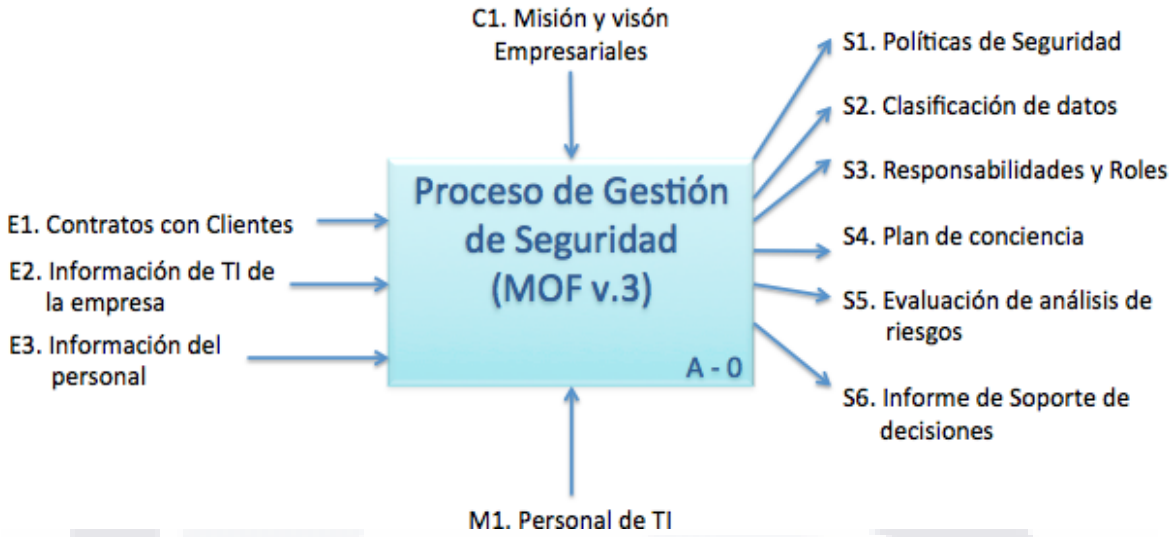


Figura 18 Proceso de Gestión de la Seguridad basado en MOF v3

Tabla 4 Aportaciones de los casos similares al Proceso de gestión de TI.

IT security standardisation	Implementing enterprise security	Information security incident response	Security standardization in incident management:
La importancia que tiene en la actualidad tener un estándar sobre todo en tema tan crucial como lo es la seguridad en TI así como distintos puntos que se deben tomar en cuenta en el ámbito mencionado.	Tomar en cuenta para la creación del proceso: • Organización (Políticas y Procesos). • Sistema Operativo. • Sistemas de gestión de base de datos (DBMS). • Telecomunicaciones. • Acceso - activos de información.	La importancia de los roles, una correcta y especifica definición estos mismos desde sus tareas hasta sus responsabilidades . De igual forma el contar con un plan de incidentes y respuestas a estos.	Menciona que se debe tener una clasificación de los accidentes que pueden suceder y principalmente un plan de cómo enfrentar dichos accidentes.

Tabla 5 Criterios de las bases para el Proceso de gestión de TI para el enfoque en Pymes.

ISO 20000	MOF 3	ITIL v2
+ Claro ciclo de vida + Estructura general del proceso + Completo	+ Manejo de riesgos + Claridad del proceso + Buena documentación	+ Conciso + Manejo general de riesgos + Simple
- Falta de Roles - Información general, no detallada - Falta de claridad en el tema de riesgos	- Nivel alto de complejidad - Gran numero de roles - Muy Extenso	- Detalles del proceso a nivel moderado - Faltan detalles específicos en manejo de riesgos - Falta de especificación de roles

Con respecto a los casos similares las contribuciones que se lograron obtener de ellos son valiosas y variadas, el Dr. Walter Fumy nos recomienda que además de tener normas de seguridad dentro de la organización estas deben de estar al día, es decir las normas deben de ir evolucionando conforme al tiempo y la tecnología, donde dichas normas su punto fundamental es llegar a evitar o en un caso no optimo por lo menos limitar el daño de algún riesgo posible tomando en cuenta que dichos riesgos de seguridad pueden ser ocasionados por nuestro mismo personal al hacer un mal uso del sistema de TI y comenta que el verdadero desafío es establecer los procedimientos adecuados, la gestión y los controles para lograr la gestión de seguridad.

Para el caso de estudio de Ken Doughty se menciona la seguridad de la información donde da a resaltar que la información es un activo importante y primordial para una organización y que al tener dicha información en el sistema este debe mantener la integridad de ella, por lo cual para seguridad debemos también tomar en cuenta todos los canales de distribución que utilizamos para llevar esta información por todo el sistema de la organización como lo es desde las vías físicas es decir el área de redes de computación

hasta los sistemas que la manipulan que van desde los correos electrónicos hasta los mismos sistemas operativos que podemos tener.

Con el articulo del Dr Abiola Abimbola se logro comprender la importancia de la respuesta a incidentes, así como la definición clara y precisa de los roles y las responsabilidades del área de gestión de la seguridad dentro de la organización, otro fundamento que nos dio es que se deben conocer los riesgos que se tienen en la seguridad, estos riesgos son los que amenazan o pueden dañar tanto el servicio de TI como la información con la que se cuenta, esto ayuda a la creación de mecanismos adecuados para la respuesta a los posibles incidentes logrando con esto poder evitar o mitigar el daño que estos pueden provocar en los distintos escenarios.

En caso relacionado con ITIL denota el interés de poder mantener nuestros servicios continuos, esto relacionado con los incidentes que pueden llegar a interrumpir nuestros servicios donde se comenta que lo que se debe buscar es llegar a conocer dichos incidentes para de esa forma se planifique la forma de reducir al mínimo el suceso de interrupciones causadas por fallas en el área de TI, una aportación final del caso es la denominación de 4 factores trascendentales en el área de gestión de seguridad los cuales serian la organización como tal, el personal, la tecnología y los procesos de la organización.

IV. Diseño Conceptual del Proceso de Gestión de Seguridad de Servicios de TI

Para cumplir los objetivos del presente trabajo así como la elaboración del diseño del modelo conceptual del proceso de gestión de seguridad se llevaron a cabo algunas tareas básicas como:

Revisión de 3 metodologías de ITSM (ISO 20000, ITIL v2 e MOF v3), enfocándonos en el Proceso de Gestión de Seguridad en cada uno de ellos.

Revisión de herramientas de software de apoyo open source.

Recopilación de información de la infraestructura del LabDC-UAA.

Simultáneamente se revisó una técnica de modelado de funciones: IDEF0, que es una herramienta sencilla pero eficiente, capaz de explicar procesos complejos de forma sencilla de comprender. Así pues para resumir el trabajo realizado durante el desarrollo de la tesis y obtener el diseño del modelo de la metodología la cual se propone más adelante, se realizó un proceso como se observa en el siguiente diagrama de contexto A-0 (a menos cero). El diagrama muestra de la manera más general (de alto nivel) el trabajo realizado durante el desarrollo de esta tesis modelada de acuerdo al estándar IDEF0.

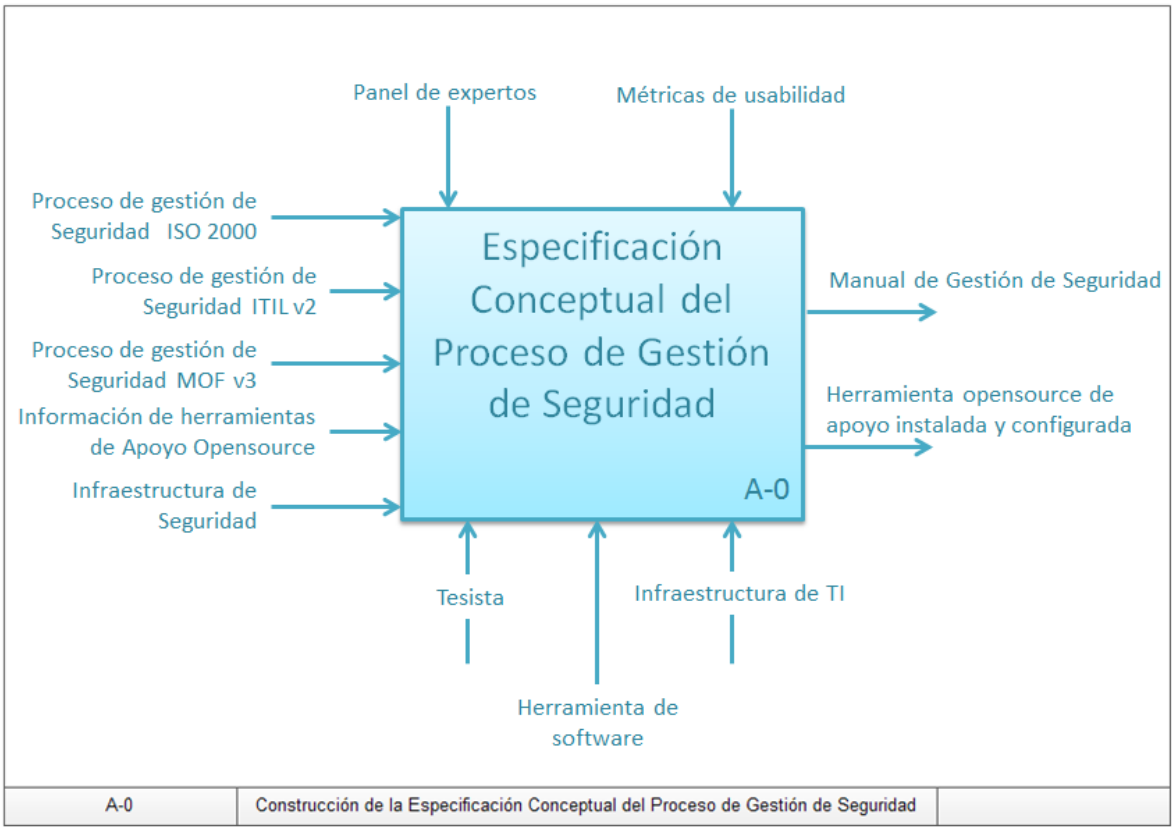


Figura 19 Trabajo realizado en esta tesis modelado con IDEF0

4.1 Construcción de la Especificación Conceptual del Proceso de Gestión de Seguridad

Se presenta el modelo con un diagrama de alto nivel en el que se muestra el tema, que para este trabajo es crear la Especificación Conceptual del Proceso de Gestión de Seguridad de TI y a partir de este nivel se irá desglosando hasta mostrar una especificación teórica de como llevar a cabo un Proceso de Gestión de Seguridad de TI básico y bien estructurado. Se mostrará paso a paso, cada uno de los procesos y tareas que se deben tomar en cuenta para la realización de esta especificación y dentro de cada proceso también se especifican las entradas, salidas, controles y mecanismos de estos. Así entonces, basándonos en los estudios previos de los estándares ISO 20000, ITIL v2 y Mof v3 y aplicando IDEF0 se propone la siguiente metodología.

En el primer paso (Figura 20) se modela de manera general el proceso de gestión de seguridad propuesto mediante el diagrama A-0, que incluye también las entradas, controles, mecanismos y salidas que se podrán obtener, posteriormente se muestra el interior del diagrama A-0 en un primer nivel de detalle (Figura 21), donde se muestran también los esquemas detallados de cada uno de los procesos clave propuestos (Planeación y Organización de Gestión de Seguridad, Gestión Operativa de Seguridad, Gestión de Control y Reportes), en cada uno de ellos se describen las tareas a desarrollar para lograr obtener las salidas/productos necesarios para llevar a cabo el proceso de gestión de seguridad propuesto.

4.1.1 Diagrama IDEF0 de Alto Nivel del Proceso de Gestión de Seguridad

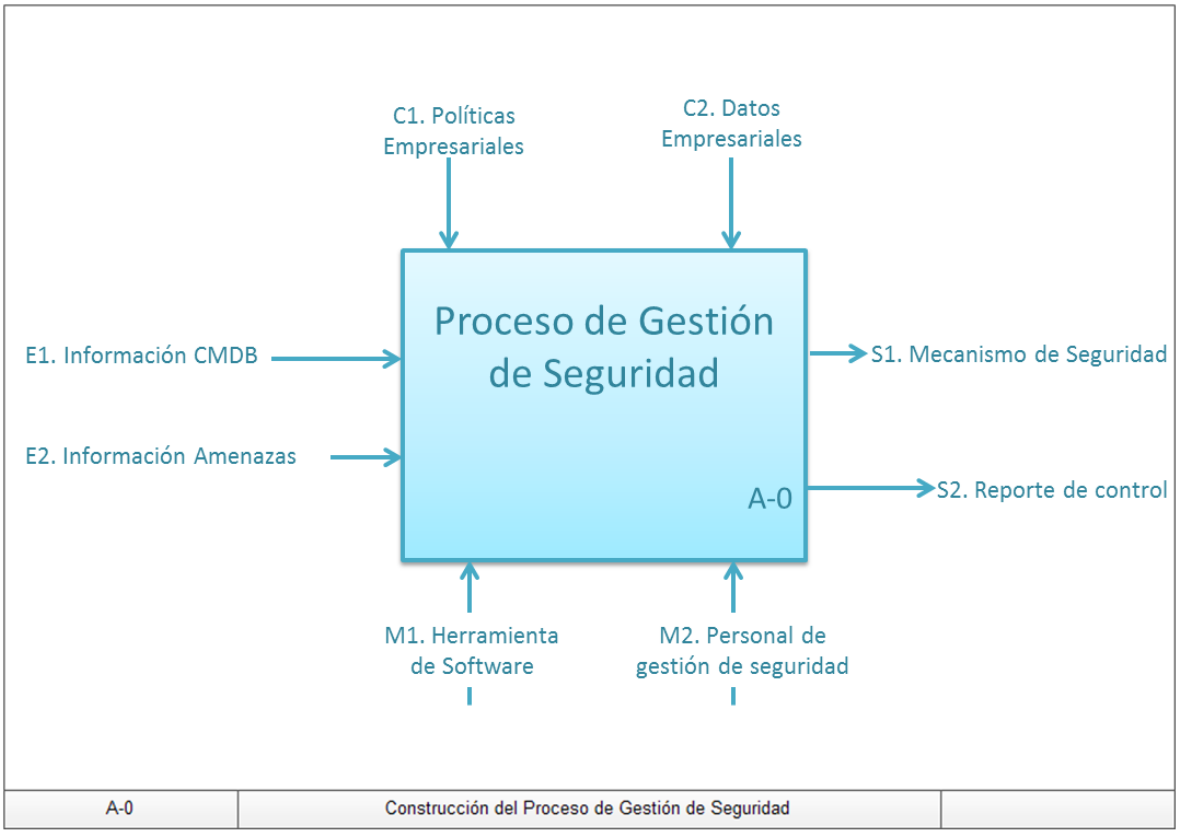


Figura 20 Diagrama IDEF0: Alto Nivel

4.1.2 Diagrama IDEF0 de Primer Nivel de Detalle del Proceso de Gestión de Seguridad

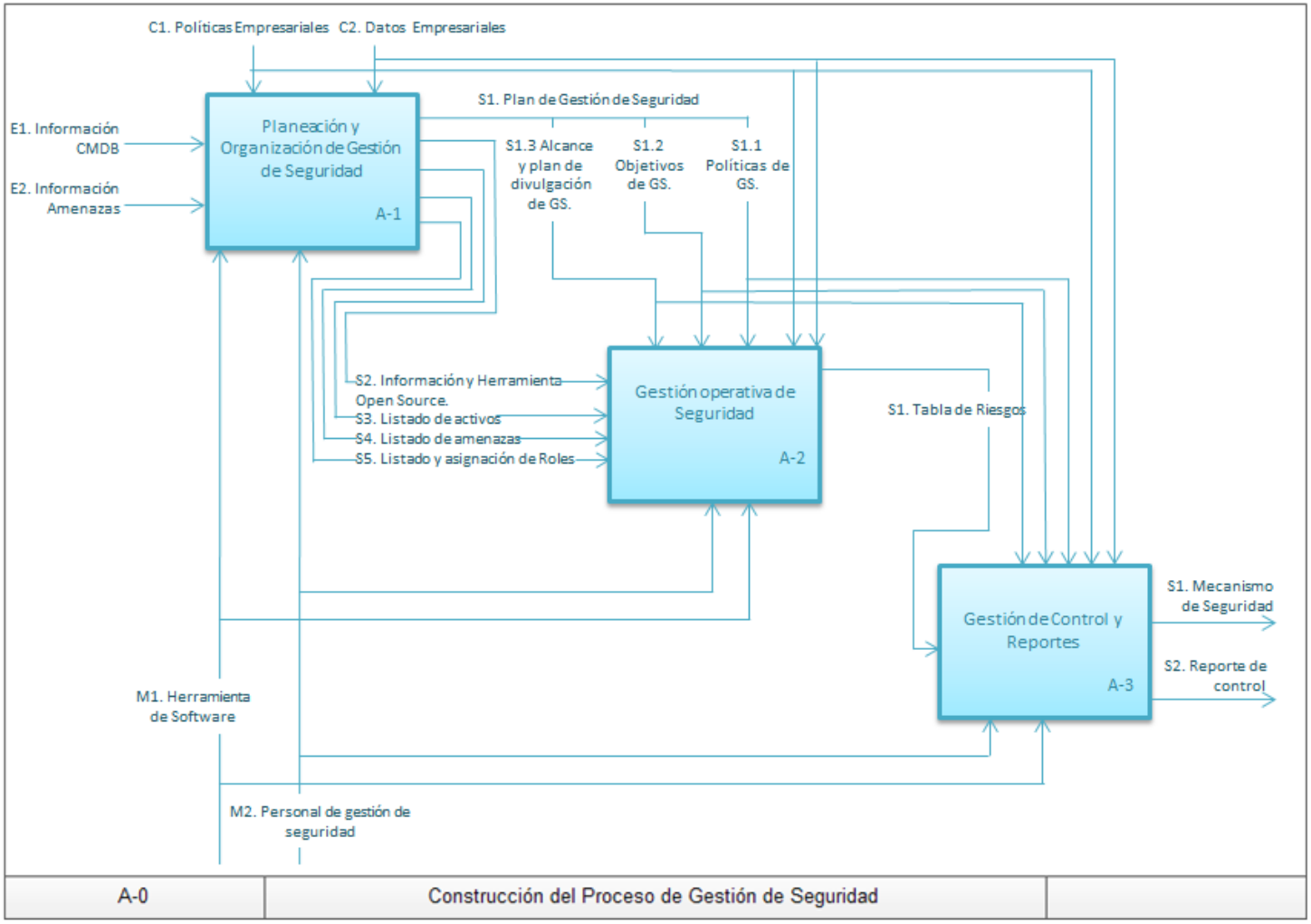


Figura 21 Diagrama IDEF0: Primer Nivel de Detalle

4.1.3 Esquema IDEF0 Detallado del Proceso A-1. Planeación y Organización de Gestión de Seguridad

Control		
C1. Políticas Empresariales. C2. Datos Empresariales.		
Entradas	**Funciones**	**Salidas**
E1. Informe de CMBD. E2. Informe de amenazas.	El propósito es definir políticas, roles, alcance y plan de divulgación de gestión de seguridad, establecer la estructura de gestión de seguridad de manera formal así como la herramienta de apoyo, mediante las siguientes funciones: **1. Definir objetivos y políticas.** **2. Definir el alcance.** a. Establecer el alcance (hasta que nivel queremos dar seguimiento). Se recomienda limitarlo por servicio a fin de que sea más sencillo de comprender. 3. **Definir Plan de divulgación.** 4. **Definir roles que intervendrán en el proceso y su asignación**, se sugieren al menos: • Coordinador de Seguridad: encargado de registrar los activos y da mantenimiento de datos a la CMDB. • Responsable de Seguridad: es el responsable de la calidad de los datos. • Auditor: encargado de verificar la integridad de la información. 5. **Definir la lista de los activos,** los cuales estan relacionados o son de importancia para la gestión de seguridad(Tabla 6). 6. **Revisar herramienta de software de apoyo disponible** (Anexo A) 7. **Definir la lista de riesgos**, crear (Tabla 7).	S1. Plan de Gestión de Seguridad. S1.1 Políticas de Gestión de Seguridad. S1.2 Objetivos de Gestión de Seguridad. S1.3 Alcance y plan de divulgación de Gestión de Seguridad. S2. Información y Herramienta Open Source. S3. Listado de activos. S4. Listado de amenazas. S5. Listado y asignación de Roles
Mecanismos		
M1. Herramienta de Sw. M2. Personal de seguridad en TI.		

Para lograr iniciar con la Gestión de Seguridad se solicitan dos entradas al proceso de las cuales se proporciona una guia base en las cuales basarse:

1.- E1. Informe de CMBD: (basado en ITIL CMBD son las siglas en ingles de Configuration management database, el propósito de esto es una base de

datos que contenga detalladamente los detalles relevantes de cada CI (ítem/elemento de configuración).

De Itil se extrajeron diferentes tipos de ítems de una organización los cuales pueden ser:

- Hardware
- Software
- Comunicaciones / Redes
- Documentación
- Personal (empleados y contratistas)

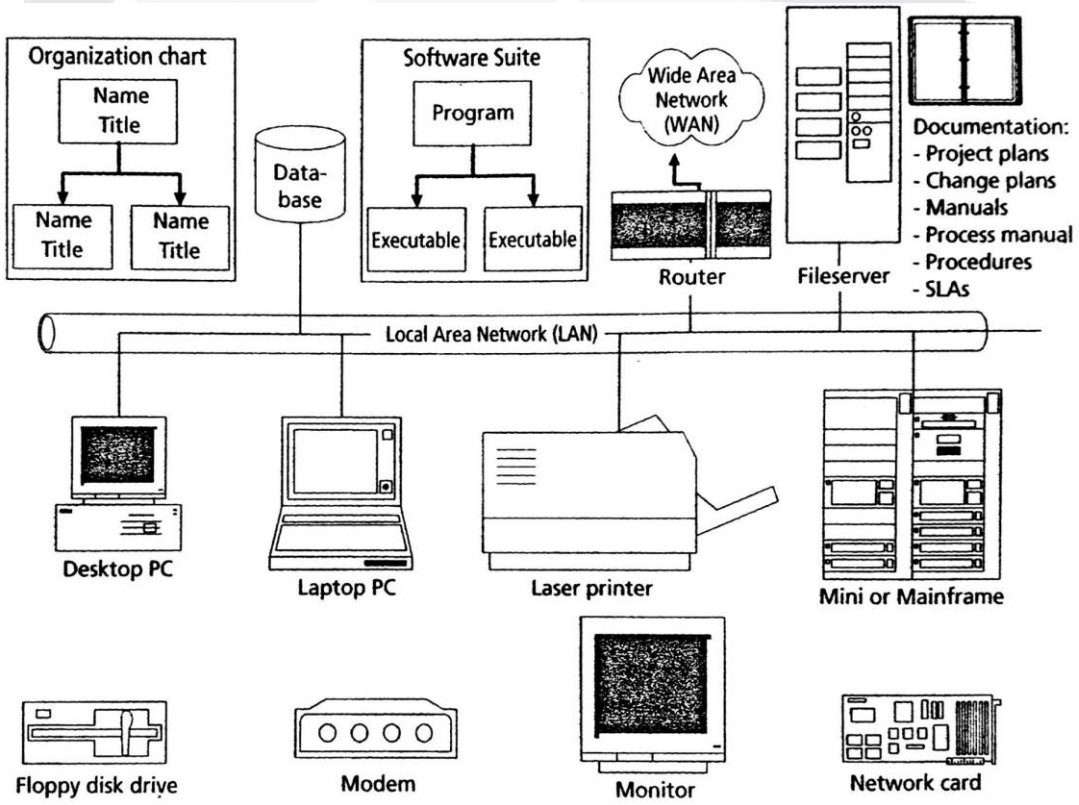


Figura 22 Ejemplo de ITIL de configuración de Ítems (ejemplo tomado de ITIL)

2.- E2. Informe de amenaza: Existen diversos tipos de riesgos posibles, se basara en dos principales raíces de las cuales cada una tiene sus propias ramificaciones (dicha clasificación de riesgos fue una aportación del Dr. Manuel Mora para este proceso de Gestión de seguridad):

Externos:

- Físicos: en este caso son los actos de la naturaleza que pueden llevar a ocasionar algún daño en el servicio o directamente en la infraestructura.
  - Lluvias
  - Terremotos
  - Incendios
  - Explosiones volcánicas
  - Tsunamis
  - Huracanes

- Organizacionales: Son las leyes o reglamentos que pudieran afectar o limitar nuestros servicios.

- Flexibilidad de TI (Proveedores): estos son problemas que pueden tener nuestros proveedores los cuales afectarían de alguna forma a nuestra organización. Estos pueden ser luz, agua, gas, drenaje, internet, telefonía, reparaciones, entre los diferentes proveedores que puede manejar la organización.
  - Suspensión de servicio
  - Pausa del servicio
  - Mal servicio o insuficiencia del mismo

Internos:

- Personal de TI: en este caso son los accidentes o riesgos que pueden ser causados debido al personal de la organización ya sea accidentalmente o premeditado.
  - Errores en el servicio
  - Caídas del servicio
  - Perdida de información
  - Alteración de información
  - Hurto de información
  - Mal funcionamiento de Hardware y Redes
  - Descompostura de Hardware o Redes
  - Perdida parcial o total en Hardware o Redes

  Esto puede ser causado por :
  - Falta de control de contraseñas (sistema, correos, etc.)
  - Falta de control de acceso (lógico y físico)
  - Falta de control de personal (credencialización)
  - Falta de control de procesos (definición de alcances)

  También se debe tomar en cuenta que puede pasar en caso de accidentes despidos o circunstancia fatales.

- ICT (Hardware, Software, Red): ICT (Information and communications technology) este punto se centra en la pérdida o daños físicos de la infraestructura de TI de la organización y en segundo grado de perdida o daños lógicos del sistema o sistemas. Este punto tiene relación con el de Personal de TI.
  - Uso inadecuado de un servicio
  - Uso Inadecuado del Hardware
  - Uso inadecuado de la de red de comunicación
  - Falta de capacitación
  - Falta de especificación de manejo de equipo
  - Deterioro de Hardware
  - Deterioro de la red
  - Actualizaciones de Software
  - Eliminación o bloqueo de Software
- Infraestructura: el mencionar infraestructura en este punto es para localizar los riesgos que pueden pasar si se descuida o fallan lo que es la infraestructura de la organización, nos referimos a esta como paredes, techos y suelos, desde otro punto de vista también se contemplan la de los servicios como son tubos de agua, conductos de gas, cableado eléctrico, fontanería, entre otros.
  - Ruptura de tubo de agua
  - Ruptura de conductos de gas
  - Ruptura de conductos de fontanería
  - Ruptura de ventanas
  - Corto circuitos en la red eléctrica
  - Caída de muros
  - Caída del techo
  - Deslave del suelo
  - Fallo del sistema de calefacción

Cabe mencionar que los previamente descritos son una base, es decir, no se menciona el 100% de los riesgos existentes o posibles, los cuales pueden variar dependiendo de la organización y el tiempo.

Para la salida S.2 Información y Herramienta Open Source, se puede observar en el siguiente capitulo las discusión de los 3 Open Source investigados a utilizar como apoyo o base para el proceso de gestión de seguridad, en dicho capitulo se decidió el uso del programa PROAct es por ello que el proceso se enfoca en el uso exclusivo de dicho software, el manual de uso y funcionamiento mas detallado se puede observar en (Anexo A).

En el diagrama de nivel detallado (Figura 21) podemos observar que para Gestión de seguridad uno de los puntos centrales es la relación con los activos de la Organización es por ello que se propone la creación de 3 tablas :

- Lista de Activos
- Lista de Amenazas
- Reporte de continuidad

Donde la primera tabla es un listado de los activos que se tienen en la organización y están relacionados con la gestión de Seguridad y puedan tener algún tipo de riesgo el cual afecte directamente su productividad o el proceso en el que se utilice o relacione dicho activo, es por ello que el primer paso es lograr identificar todos los activos con riesgos relacionados a las TI.

Tabla 6 1# Lista de Activos

ID	Tipo	Activo	Valor económico	Utilidad	Antigüedad
A.1					
A.2					
….					
A.K					

Donde los campos de los tabla Listas de Activos se refieren a :

- *ID*: será el identificador único.

- *Tipo*: Donde los activos pueden tener diferentes orígenes como:
    1) Software
    2) Hardware
    3) Datos
    4) Personal (tanto por su trabajo como por su expertise o conocimiento)

- *Activo*: El nombre o descripción sencilla del activo de la organización.

- Valor económico: este campo expresa el coste o monto monetario del valor del activo, sus posibles rangos son:
    1) A (Alto) : cientos de miles de pesos.
    2) M (Medio) : miles de pesos.
    3) B (Bajo) : cientos de pesos.

- Utilidad: dicho campo expresa el grado o valor de contribución que otorga o afecta en los servicios o procesos de la organización dicho activo.
    1) A (Alto) : fundamental
    4) M (Medio) : básico o media
    5) B (Bajo) : casi nulo o nulo

- Antigüedad: es en relación a la antigüedad del activo es decir el tiempo de vida útil del mismo, sus posibles casos serian:
    1) N (Nuevo)
    2) M (Medio)
    3) V (Viejo)

Teniendo los Activos identificados, se prosigue con la identificación de las amenazas las cuales pueden afectar los activos que previamente se identificaron, para la creación de la segunda tabla se deben tomar en cuenta que existen diferentes tipos de Amenazas o indecentes como lo pueden ser

Naturales, por el Personal o tanto el Software y Hardware, donde debemos relacionar cada una de las amenazas con los activos que ya se tienen listados previamente. Usar como base la entrada E2. Informe de amenaza, para la selección de los riesgos posibles.

Antes de empezar con la siguiente tabla es importante tener en cuenta las definiciones de: (obtenidas del Curso de Control de Riesgos Del Dr. Manuel Mora)

1) *RIESGO*: es un evento que puede suceder (donde es posible o no estimar su probabilidad de ocurrencia) con consecuencias negativas (perdida o disminución de un recurso valioso).
2) *AMENAZA*: es una fuente causante o co-generadora de riesgos.
3) *PROBABILIDAD DE RIESGO*: es un valor numérico u ordinal (calculado o estimado) de la frecuencia de ocurrencia del riesgo.

Tabla 7 2# Lista de Amenazas (Primer parte)

ID	Categoría	Fuente de Amenaza	Acciones Dañinas
R.1			
R.2			
…			
R.t			

Donde :

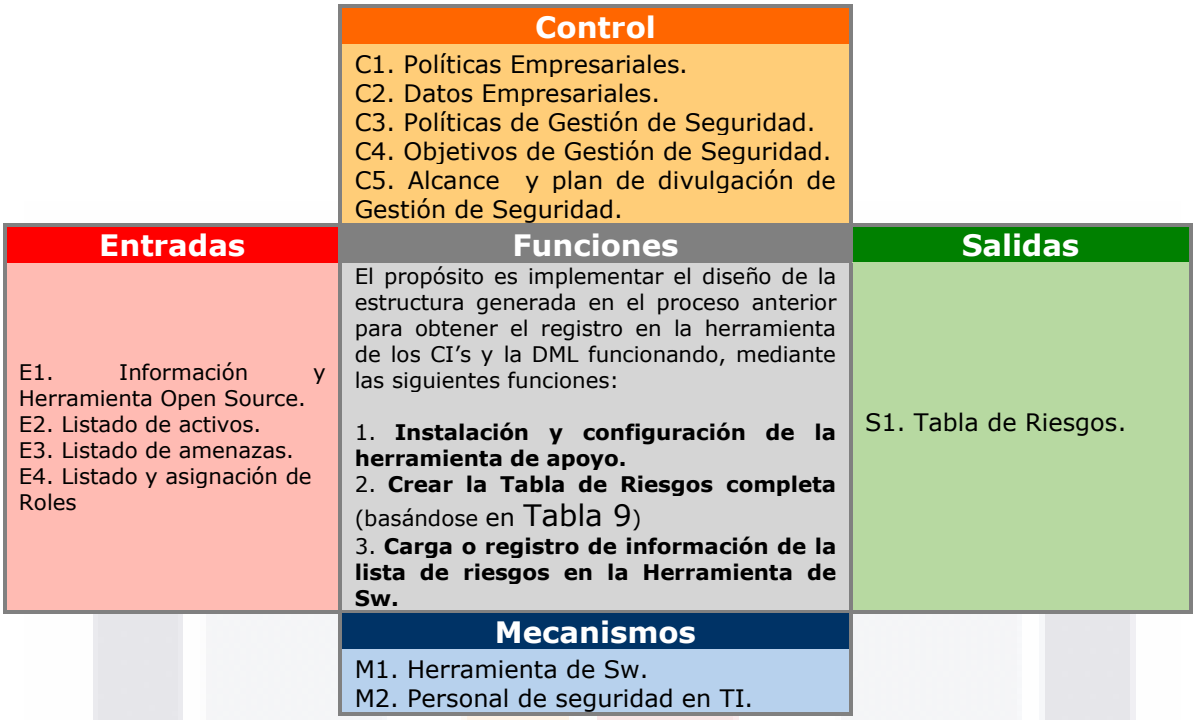
- ID: será el identificador único.

- Categoría: se nombra el tipo de amenaza o incidente que puede suceder y provocar alguna afectación relacionada con TI (ejemplo Naturales, Personal, Software o Hardware).

- Fuente de Amenaza: se indica en especifico la causa o el causante de la posible amenaza o incidente que puede suceder (ejemplo en el caso de Naturales: terremotos, lluvias, huracanes).

- Acciones dañinas: en relación a la fuente de amenaza este indica la acción especifica de riesgo (ejemplo para el caso de fuente de amenaza en la lluvias una acción dañina podría ser la lluvia excesiva causando filtraciones o inundaciones en el recinto).

4.1.4 Esquema IDEF0 Detallado del Proceso A-2. Gestión operativa de Seguridad



En la tabla de Listas de Amenazas se le agregaran nuevos campos :

Tabla 8 2# Lista de Amenazas (Completa)

ID	Categoría	Fuente de Amenaza	Acciones Dañinas	Activos Afectados	Daño	Probabilidad	Exposición al Riesgo
R.1							
R.2							
…							
R.t							

- Activos Afectados: Donde se mencionaran los activos afectados directamente por las acciones dañinas.

- Daño: los valores posibles serán (A)Alto, (M)Medio (B)Bajo el cual indica el daño posible o el grado de afectación a la organización.

- Probabilidad: es la posibilidad con la cual puede ocurrir dicho percance, sus valores pueden ser:

(A) Alto: Prácticamente algo que es probable de suceder (P >= 80%)

(M) Medio: Prácticamente algo que puede suceder (P entre 40% a 60%)

(B) Bajo: Prácticamente algo que sucede con poca frecuencia (P <= 20%)

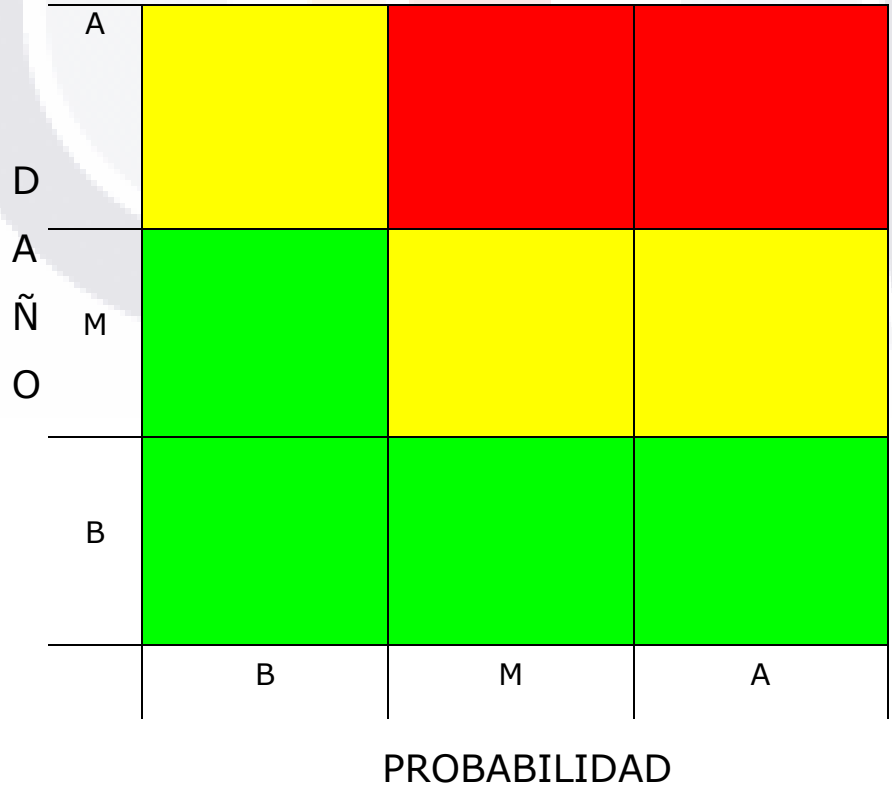
- Exposición al Riesgo: La exposición al riesgo es la combinación entre el daño y la probabilidad de la amenaza misma, pueden tomar 3 distintos valores donde indican (los valores posibles entre las diferentes combinaciones entre daño y probabilidad se pueden ver claramente en la tabla de Reporte de Continuidad y mas detalladamente):

(V) Verde : Nivel de exposición al riesgo Bajo

(A) Amarillo : Nivel de exposición al riesgo Medio

(R) Rojo : Nivel de exposición al riesgo Alto

Tabla 9 3# Reporte de continuidad



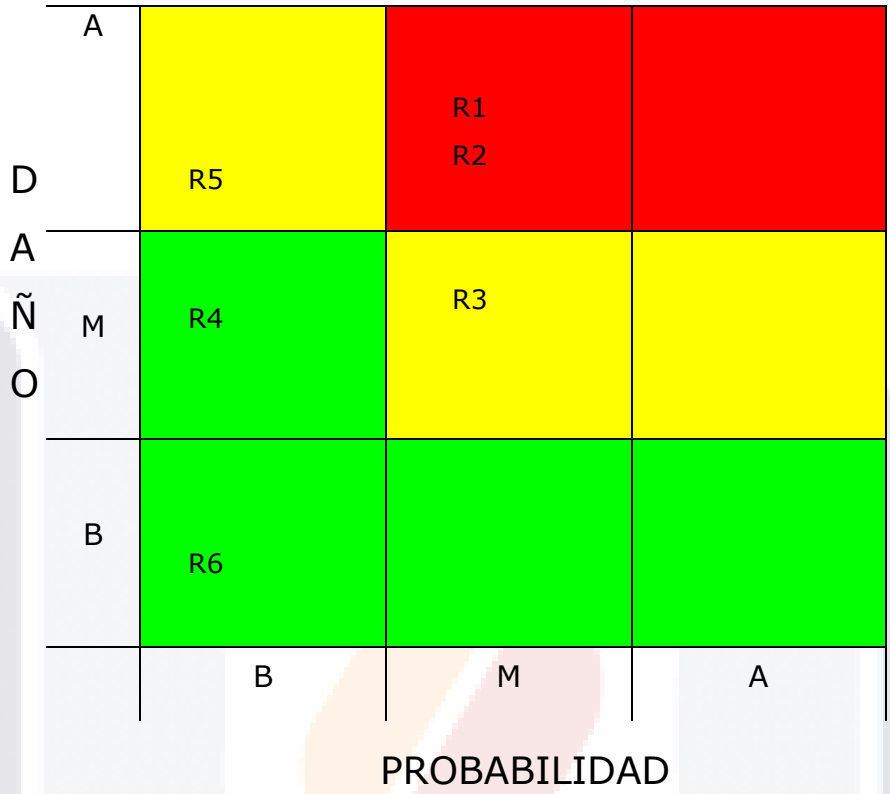
Se toma como base la tabla Lista de Amenazas donde ya una vez que se tiene identificado tanto los activos como las amenazas se procede a generar la tabla de Reporte de continuidad donde lo que se busca en ella es poder identificar los puntos críticos los cuales se deben analizar según su daño y la probabilidad con la cual puede suceder.

Donde se encuentran 3 valores:

a. Verde : prioridad baja o nula, estos incidentes pueden ser los últimos a resolver o incluso puede llegar a ignorarse.
b. Amarillo : prioridad media, en este caso serán estudiados y se buscara la forma de resolver o mitigar el daño posible, estos pueden incluso resolverse en tiempos medianamente futuros.
c. Rojo : prioridad alta, estos serán los de mayor importancia y atención, donde se buscara la forma de resolver o mitigar pero en tiempo inmediatos y demasiados cercanos, otra opción es ver la forma de poder atacar el problema quizás sin llegar a resolverlo por completo pero poder reducir considerablemente su afectación o hasta algún cambio en el sistema o proceso que este afecte.

La interacción que hay entre la tabla Lista de Amenazas y Reporte de continuidad es fundamental debido a que los puntos a controlar los podremos verificar en la tabla de Reporte de Continuidad mas sin embargo estos puntos son los que tenemos como resultado en la primer tabla mencionada previamente donde se hace el cruce de los activos y amenazas, las cuales se clasifican según sus valores finales como pueden ser Verde, Amarillo y Rojo. Un ejemplo de esto es mostrado mas adelante (Tabla 10 Ejemplo de 3# Reporte de continuidad). Según el valor que se obtenga de cada Riesgo de dicha tabla será la forma en la cual ser abordaran tanto en forma o tiempo esto debido a que lo que se buscara analizar e intentar resolver primero los que cuenten con efectos importantes bien sean en el sistema o proceso en el cual interactúan y cuenten con una probabilidad alta de ocurrir.

Tabla 10 Ejemplo de 3# Reporte de continuidad



En este punto del proceso es donde se vinculara los datos que se tienen con el uso del software de apoyo, esto mediante la introducción de los datos al mismo. Para lograr introducir los valores requeridos se deben seguir los pasos del Anexo A: 1. Inicialización (Completo) y 2. Captura de Situaciones (Riesgos) y Acciones contra Riesgos (Paso 2.1 y 2.2).

Para lograr optimizar el uso de la Herramienta de apoyo será necesario crear la tabla de Daños residuales en la cual se observaran los cambios en los riesgos estos pueden afectar tanto el daño como la probabilidad, estos cambios o diferencias son dados según las modificaciones que generemos en nuestro sistema o procesos para lograr afectar dichos riesgos intentando con esto minimizar los mismo buscando obtener un menor índice de criticidad, por lo cual según la medidas que se hayan tomado se reduzca el daño o la probabilidad original de los riesgos. Esto se logra debido a las contramedidas

seleccionadas, también se debe indicar el coste de la aplicación de la contramedida. A que nos referimos con contramedidas, serán las acciones que tomaremos para cada una de las amenazas teniendo 5 tipos específicos de contramedidas (clasificación tomada del Curso de Gestión de Riesgos del Dr. Mora):

1) C.1: IGNORAR • ACEPTAR • RETENER RIESGO SIN CONTRAMEDIDAS: en caso de riesgos evaluados a nivel BAJO, es posible esperar que nada suceda.

2) C.2: EVADIR RIESGO: en caso de riesgos de nivel ALTO, donde los costos no sean razonables, pero sin embargo sea posible modificar algunas condiciones de la organización, para no incurrir en la situación de riesgo analizada. Al tomar otro curso de acción es posible un Incremento en costo del proceso (e.g. menor o Iguala 20%), o cambio en calendario o funcionalidad razonable.

3) C.3: TRANSFERIR RIESGO: en caso de riesgos de nivel ALTO, donde los costos de transferencia a otra entidad sean razonables, o de nivel MEDIO donde los costos de transferencia sean muy bajos. En el primer caso se espera un posible Incremento en costo del proceso razonable (e.g. menor o Igual a 20%).

4) C.4: MITIGAR RIESGO (PREVENIR, MONITOREAR): en caso de riesgos MEDIO o ALTO, donde la organización tiene recursos suficientes para atacarlo. Se espera un posible incremento en costo del proyecto razonable (e.g. menor o igual 20%).

5) C.5: ACEPTAR RIESGO CON PLAN DE CONTINGENCIA: en caso de riesgos de nivel ALTO, que no puedan ser atacados o transferidos por altos costos, es sugerido el planear acciones de recuperación. No obstante, también se espera un posible incremento en costo del

proyecto razonable (e.g. menor o Igual a 2046), aunque de suceder, habrá costos más fuertes dado su ocurrencia.

Cada contramedida tiene sus propias acciones posibles especificas:

1) IGNORAR • ACEPTAR • RETENER RIESGO SIN CONTRAMEDIDAS:
- Ac.1: Comunicar alerta de riesgo al equipo
- Ac.2: Omitir cualquier comentario sobre posible ocurrencia
- Ac.3: Solicitar un esfuerzo extra pero normal al equipo

2) EVADIR RIESGO:
- Ac.1: Negociar la cancelación o eliminación del factor critico
- Ac.2: Negociar un ajuste sobre el funcionamiento del factor critico
- Ac.3: Negociar un cambio sobre la tecnología en particular usada en el factor de riesgo
- Ac.4: Evitar conformar un quipo de trabajo con conflictos a pesar de alto expertise
- Ac.5: Evitar nuevos proyectos durante el desarrollo del actual

3) TRANSFERIR RIESGO:
- Ac.1: Sub-contratar una organización externa para el cumplimiento de un factor funcional critico
- Ac.2: Adquirir un seguro (mas usual para asegurar el reemplazamiento de equipos computacionales críticos de alto costo)
- Ac.3: Contratar dictaminador externo experto para evaluar la factibilidad de un factor critico (en este caso se espera que el dictamen sugiera un cambio)

4) MITIGAR RIESGO (PREVENIR, MONITOREAR):
- Ac.1: Invertir en entrenamiento adicional
- Ac.2: Invertir en tecnología critica adicional
- Ac.3: Invertir en recursos humanos expertos adicionales

- Ac.4: Invertir mas presupuesto en hrs-expertise con el mismo equipo humano
- Ac.5: Invertir en equipo alternativo humano para prototipar/analizar/negociar dicho factor
- Ac.6: invertir en componentes externos ya totalmente comprobados en su funcionalidad y correctividad
- Ac.7: Invertir en estudios especiales (simulaciones, benchmarking, performance analysis, reability analysis) con grupos expertos externos para clarificar la criticidad

5) ACEPTAR RIESGO CON PLAN DE CONTINGENCIA:

- Ac.1: Desarrollar un plan de contingencia básico (optimista, se asume que el riesgo no sucede o si sucede su impacto final es menor que el inicialmente esperado)
- Ac.2: Desarrollar un plan de contingencia extremo (pesimista, se asume que el riesgo tarde o temprano sucederá y el plan es desarrollado para actuar en consecuencia)
- Ac.3: Desarrollar un plan de contingencia moderado (realista, se asume que el riesgo sucederá pero dado su aceptación el equipo de proyecto estará preparado con un plan realista y factible para actuar en consecuencia)

Tipos de costos de contramedidas: este valor indica el monto económico que le resultara a la empresa por efectuar las acciones de las contramedidas, donde los valores posibles son: cero (Zero), bajo (Low), medio (Med) o alto (High). Es posible indicar valores intermedios: algo medio entre Lo-Med, y algo alto entre Med-Hi.

Consecuentemente que se tiene la lista de amenazas de igual forma que sus contramedidas tomadas para cada una de las mismas, se comienza con la generación de la tabla de Daños Residuales en la cual se ven los cambios tanto en daño como en probabilidad de las amenazas después de realizar su

contramedida indicada. Se continua con el uso del Software de apoyo, aplicando los pasos 2.3 y 2.4 del Anexo A, para la generación de la tabla Daños Residual.

Tabla 11 Ejemplo de 4# Daños Residuales

DAÑO				
	A	R1 R5		
	M	R3	R2	
	B	R4 R6		
		B	M	A
		PROBABILIDAD		

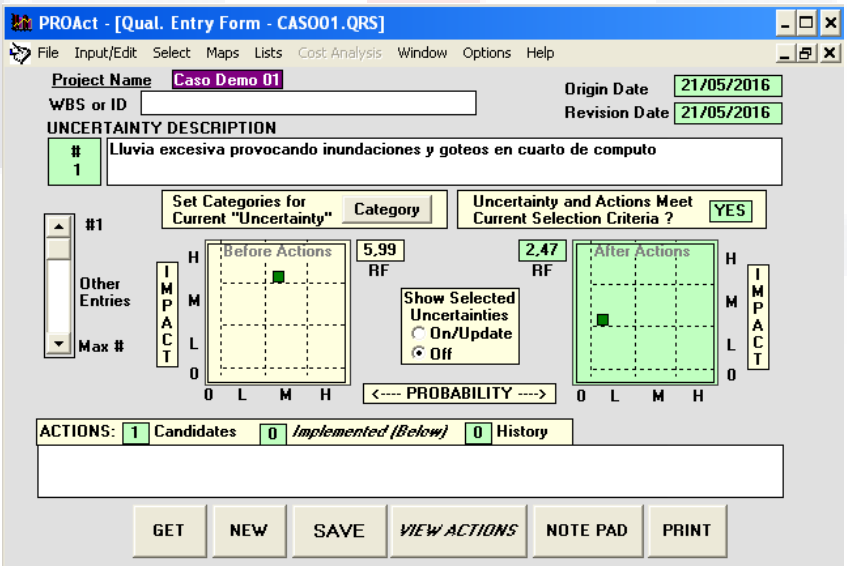
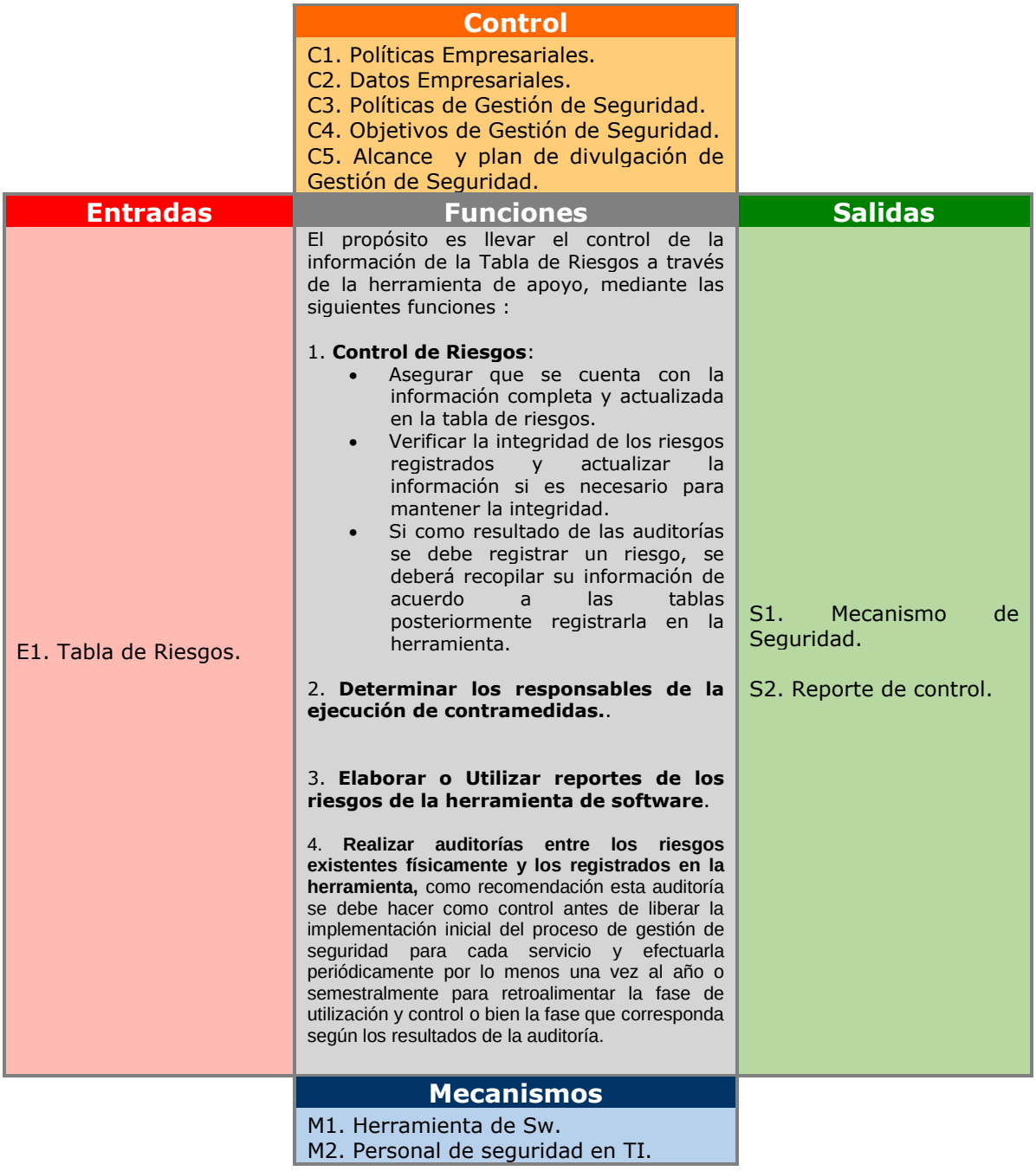


Figura 23 Ejemplo de Riesgo con valores antes y después de contramedida en el Software de apoyo.

4.1.5 Esquema IDEF0 Detallado del Proceso A-3. Gestión de Control y Reportes



Para la gestión de control y reportes se utiliza la sección 3 del Anexo A. Esto debido a que la entrada a este proceso, E1. Tabla de Riesgos debe estar en el

software de apoyo dichos datos son los que se usaran para lograr llevar el control de los riesgos y su contramedida seleccionada.

Para el seguimiento de las contramedidas se debe incluir en los reportes de control un formato donde lo que indicara será la amenaza, su contramedida y el responsable de efectuar dicha contramedida .

S1. Mecanismo de Seguridad (Formato):

La hoja de cubierta con título del informe, la fecha, y el ID del preparador

Tabla de contenido

Resumen ejecutivo

1. Introducción
    - 1.1 Políticas
    - 1.2 Objetivos
    - 1.3 Alcance
2. Descripción del Sistema
    - 2.1 Información general
    - 2.2 Lista de activos
    - 2.3 Lista de Amenazas
3. Metodología utilizada
    - 3.1 Tabla de Riesgos
4. Conclusiones
    - 4.1 Las zonas de alta vulnerabilidad
    - 4.2 Amenazas significativas
    - 4.3 Medida de cumplimiento (de contramedida requerida)
5. Recomendaciones
    - 5.1 Justificación
    - 5.2 contramedidas necesarias
    - 5.3 contramedidas discrecionales
        - 5.3.1 Costo beneficio

Apéndices como sea necesario para apoyar el informe con la información técnica. Las representaciones gráficas (la cual será con el Software) .

Este mecanismo fue tomado y acoplado del documento Risk Analysis helps establish a good security posture; Risk Management keeps it that way(B. D. Jenkins, 1998).

S2. Reporte de control: es necesario determinar el responsable de la aplicación de las contramedidas se debe entender que son procesos diferentes la ejecución de los requisitos para lograr llevar acabo las contramedidas y la revisión del seguimiento de contramedidas, es decir una acción es llevar acabo lo requerido y la otra es la revisión de lo previamente mencionado, para la revisión, el encargado de la Gestión de Seguridad es quien debe dar seguimiento de en que proceso va o si se concluyo con las acciones de la contramedida y el otro responsable será quien este encargado de ejecutar o aplicar lo necesario para efectuar dicha contramedida. Los campos del reporte deben incluir (Anexo B) :

1. ID: Amenaza
2. Acciones Dañinas
3. Daño (antes de contramedida)
4. Probabilidad (antes de contramedida)
5. Exposición al Riesgo(antes de contramedida)
6. Contramedida
7. Daño (después de contramedida)
8. Probabilidad (después de contramedida)
9. Exposición al Riesgo(después de contramedida)
10. Inicio de Acciones de contramedida
11. Fin de Acciones de contramedida
12. Responsable de acción(es)
13. Status de la(s) acción(es)
14. Revisión // fecha y nombre de quien reviso

V. Herramientas Open Source de soporte al proyecto de seguridad

5.1 Coras

CORAS es un método para la realización de análisis de riesgos de seguridad. CORAS proporciona un lenguaje personalizado para la amenaza y el riesgo de modelado, y viene con directrices detalladas que explican cómo el lenguaje se debe utilizar para capturar y modelar la información pertinente durante las diversas etapas del análisis de seguridad. El Lenguaje Unificado de Modelado (UML) se suele utilizar para modelar el objetivo del análisis. Para documentar los resultados intermedios y para la presentación de las conclusiones generales que utilizamos diagramas Coras especiales que se inspiran en UML. El método CORAS proporciona una herramienta informática diseñada para apoyar a documentar, mantener y reportar los resultados de análisis a través de modelos de riesgo.

Cuenta con la pagina http://coras.sourceforge.net/ donde su puede descargar la herramienta asi como información sobre la misma, esta misma esta disponible para distintas plataformas como lo son Windows, Linux, MacOS entre otras.

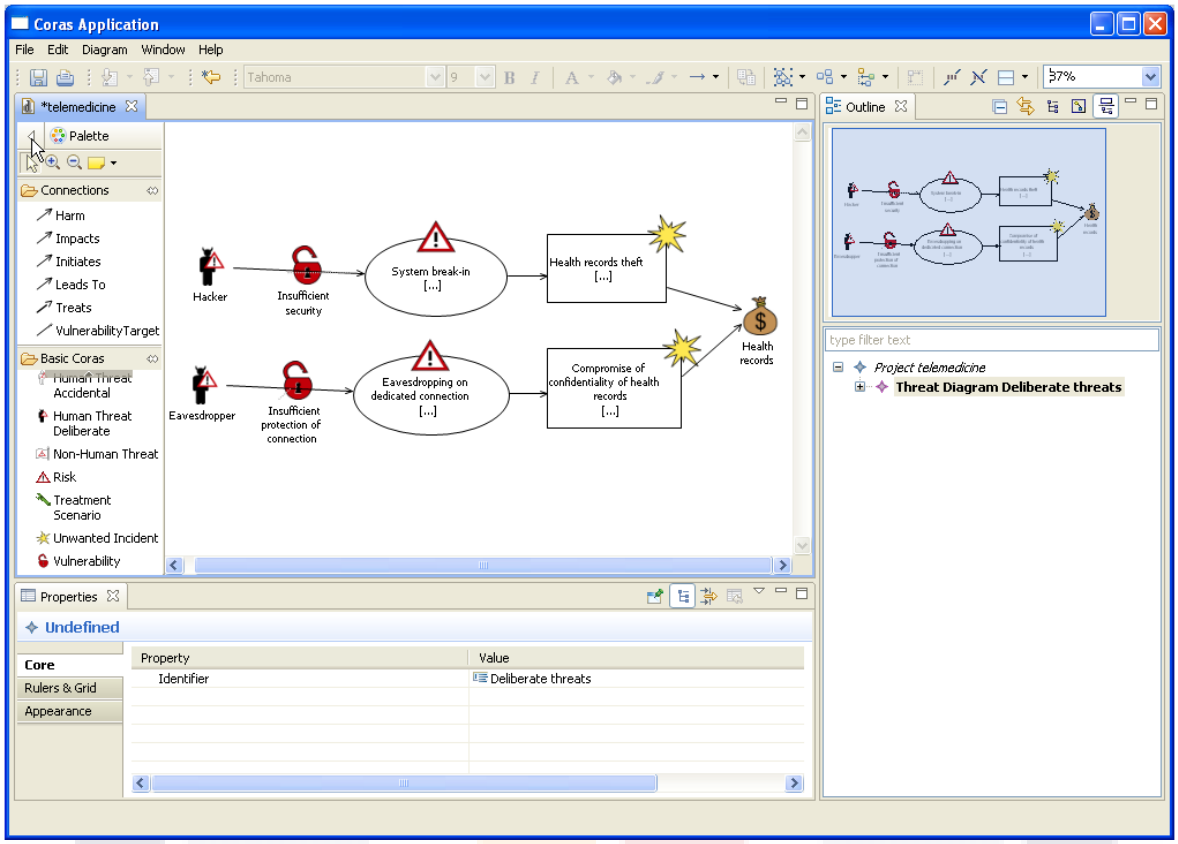
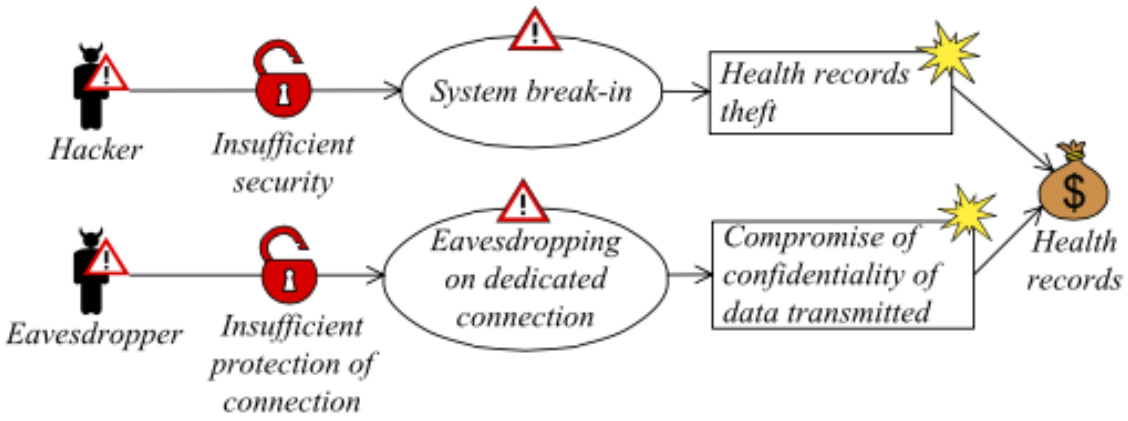


Figura 24 Ejemplo de la interface de Coras

Coras tiene como función principal la creación de diagramas estos toman en cuenta la relación que hay entre las amenazas y el sistema en general el prime paso es la identificación de la tabla de riesgo de alto nivel estos pueden variar como empleados, hacker, fallo de red o sistema entre otras, la segunda tabla que nos recomienda que generemos el la Activos donde en esta se busca obtener la totalidad de los activos con los que cuenta la organización que se podrían ver afectados por algún riesgo, una ves que se tengan estas se generara la escala de probabilidad con la que pueden suceder (donde puede usar términos como probable, no tan probable, raro y donde se le da un valor determinado a estos como puede ser que en el caso de raro es cuando ocurre una ves cada 2 años). La tabla que prosigue seria la de Consecuencias donde esta contiene el valor del daño que puede causar como la perdida de información (un ejemplo seria catastrófica: más de 1000 registros de una base de datos se ven afectado). Y para finalizar seria la tabla de matriz de

evaluación de riesgos donde por medio de un cruce de la tabla de probabilidad y consecuencia se logran distinguir las áreas de preocupación.

Lo malo es que Coras no cuenta con un área donde puedan programarse estas tablas que nos pide si no que corás se enfoca en la creación de los diagramas de los resultados de estas tablas .



5.2 Project Risk Analysis (ProjRisk)

El software Proyecto de Análisis de Riesgos (PRA por sus siglas en ingles) permite evaluar a los riesgo ser evaluados , y calcula la contingencia financiera necesaria para cubrir esos riesgos. Con demasiada frecuencia, la contingencia del proyecto se estima sin mucha consideración a los riesgos reales involucrados. El procedimiento seguido en el PRA impulsa la estimación disciplinada, y calcula la contingencia requerida utilizando el método estadístico demostrado conocido como simulación de Monte Carlo.

Aunque el software ARP utiliza sofisticadas técnicas estadísticas , se ha escrito para los que están más a gusto con la estimación y el cálculo del coste que con las estadísticas. Todos los modelos estadísticos y distribuciones requeridos se han creado específicamente para el análisis de contingencia y no se requieren conocimientos de la estadística .

Los resultados calculados por PRA se pueden visualizar en formato gráfico fácil de leer que dan forma rápida y eficaz el estimador de una valoración global de los riesgos.

Proyecto de Análisis de Riesgos y Contingencias, su versión actual se ejecuta bajo Windows XP / Vista / Win 7 / Win 8 / Win 8.1. Su pagina oficial es http://www.katmarsoftware.com/pra.htm se puede obtener en dicha liga una prueba del mismo.

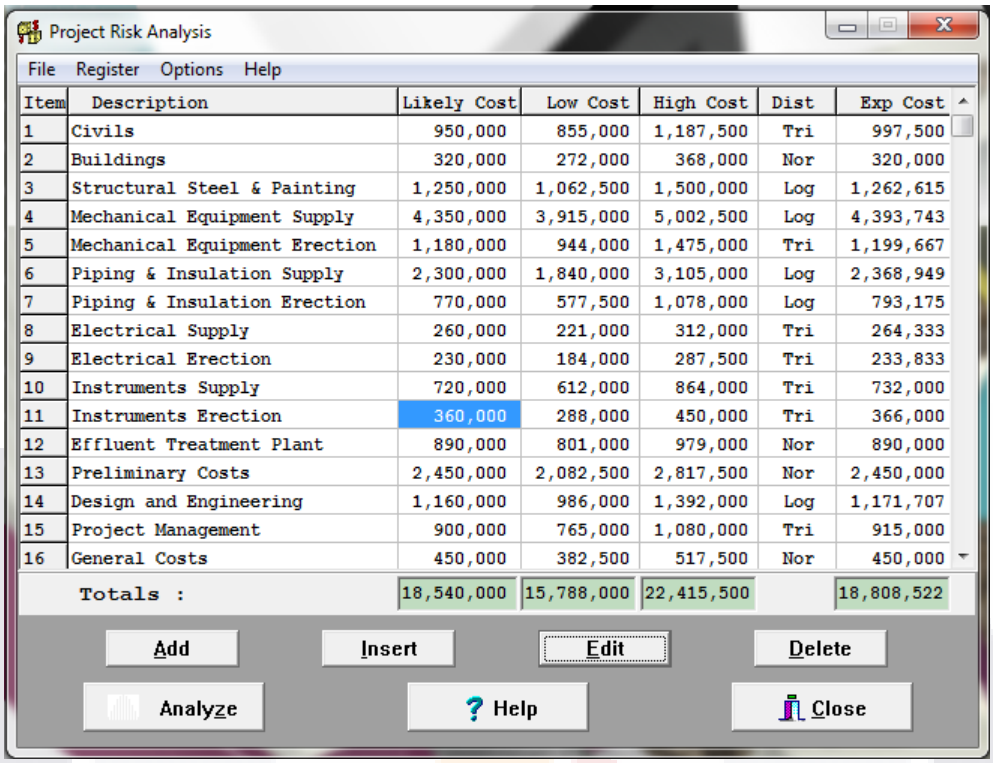


Figura 25 Ejemplo de interface primaria de ProjRisk

Project Risk Analysis muestra en su interface inicial los campos (los cuales son los valores que podemos introducir):

1. Numero de ítem (lo determina el sistema)
2. Descripción
3. Costo Probable
4. Costo Bajo
5. Costo Alto
6. Distribucion (Normal, LogNormal, Triangular)
7. Costo Exponencial

Estos valores los podemos editar o cambiar según sean nuestros requerimientos o problemas.

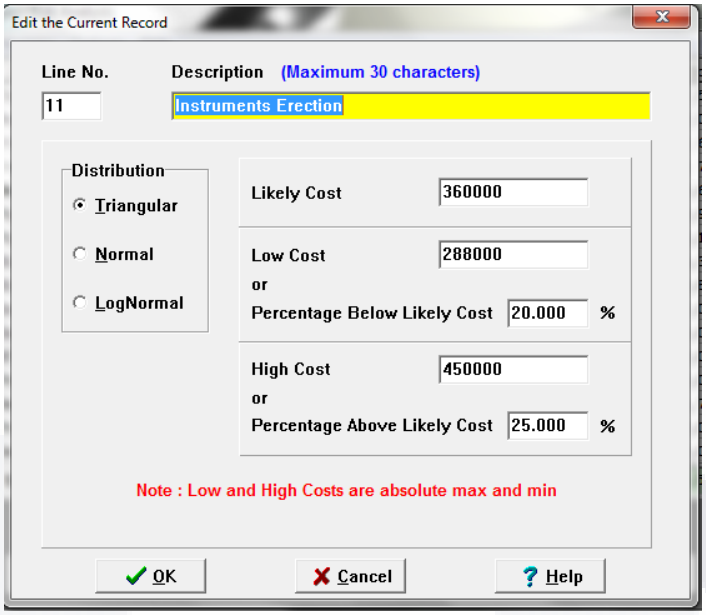


Figura 26 Ejemplo de cambio de datos en ProjRisk

Además de obtener las estimaciones de los costos y las distribuciones se especifican para cada categoría en la estimación, se pueden analizar estos valor esto mediante que todo el proyecto se simula miles de veces utilizando el método de Monte Carlo y los costos totales del proyecto se representan gráficamente en un histograma. Esto muestra claramente la gama de costos que se pueden esperar para el proyecto.

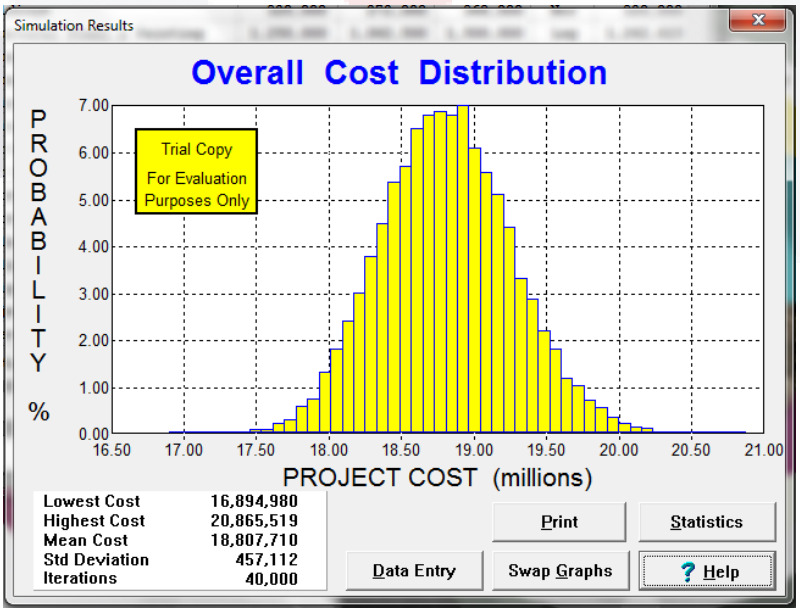


Figura 27 Ejemplo de graficas en ProjRisk

5.3 PROAct

Su nombre proviene de "PROAct " :

- **P**roactive
- **R**isk and
- **O**pportunity
- **ACT**ion

ProAct menciona que actualmente la complejidad de los proyectos es mayor y los tiempos mas ajustados. Y controlar los costes en un entorno de incertidumbre es más importante que nunca.

PROACT está diseñado para ayudar a controlar sistemáticamente las incertidumbres, riesgos y oportunidades. Dicho software es fácil de usar es una herramienta de apoyo a la toma de decisiones eficaces, que proporciona a los administradores un marco coordinado para la identificación, evaluación, seguimiento, control y presentación de informes relacionados con los riesgos y oportunidades del proyecto.

Su gestión de riesgos se centra en la comprensión y la lucha contra las siguientes cuatro dimensiones de incertidumbre: probabilidad, impacto, costo y eficacia. PROACT combina técnicas de análisis de riesgo convencionales con otros principios de gestión probadas.

PROACT formula juicios por dos métodos. El modo cualitativo no numérica acepta evaluaciones cualitativas de la probabilidad, el impacto y el coste (bajo, medio y alto).El modo numérico acepta estimaciones cuantitativas (% de probabilidad de incertidumbre e insumos para los costos de impacto y de acción). Para dar cabida a las incertidumbres de planificación, este modo

acepta estimaciones probabilísticas (distribuciones normales, triangulares o uniformes). Ambos modos cuentan con mapas que muestran el apoyo a las decisiones de acciones candidatas frente al impacto ponderado de riesgos y oportunidades.

Es una herramienta disponible para Windows XP de 32 bits, en sistemas mas recientes o sistemas como Linux no cuenta con dicha compatibilidad. Su pagina oficial es http://maxvalue.com/pabroch.htm .

Al inspeccionar las características de los 3 open source previamente mencionados y su aportación o soporte que darían al proceso de Gestión de seguridad se determino el selección de PROAct como uso de software de apoyo, es por ello que se creo el manual de uso de este software el cual se puede ver en el Anexo A, donde se especifica el uso de dicho software en relación a este proceso esto se debe a que el sistema soporta dos principales tareas las cuales son análisis cuantitativo y el análisis cualitativo para este proceso de Gestión de Seguridad en especifico se utilizara el modo cualitativo.

VI. Soporte al proceso de Gestión de Seguridad de servicios de TI usando una herramienta de open source : Caso LABDC-Uaa

Para la implementación del proceso diseñado en la sección previa se estudiaron tres herramientas open source (ver capitulo V), de las cuales debido a las características encontradas de cada una de ellas se seleccionó PROAct, debido a que es la que mejor se logro ajustar al modelo y las necesidades del LabDC-UAA. Para el caso particular del LabDC-UAA, se implementa un proyecto piloto básico, tomando como ejemplos solo algunos de los elementos de la infraestructura que se tienen debido a que cuenta con un número considerable de elementos que por cuestiones de tiempo no es viable capturar su información. Sin embargo, en trabajos posteriores al desarrollo de este proyecto piloto se podrá implementar el proceso de gestión de seguridad completo, cubriendo el 100% de los servicios ofrecidos por el LabDC-UAA. Una vez aclarada la situación, se procede a la implementación del "Proceso de Gestión de Seguridad de TI" diseñado una sección anterior (ver capitulo IV), para el LabDC-UAA, mediante el cual los alumnos de LTI y de la MITC tienen acceso a diversos cursos cortos o recursos, se pueden apreciar pantallas del servicio que se encuentra en funcionamiento accesible desde la dirección http://148.211.145.149 (Anexo D). Siguiendo la metodología propuesta, en primer lugar se presenta el diagrama A-0 de alto nivel aplicado al caso LabDC-UAA (Figura 28). Así mismo, se irán desglosando los diagramas con mayor detalle hasta aplicar la metodología propuesta para el LabDC-UAA (DataCenter).

De igual forma como complemento para la comprensión de la implementación en la herramienta open source PROAct se desarrolló un video demostrativo del uso de la herramienta como soporte al caso demo empleado, el cual puede ser consultado como se indica en el Anexo E.

6.1 Diagrama IDEF0 de Alto Nivel del Proceso de Gestión de Seguridad: Caso LabDC-UAA

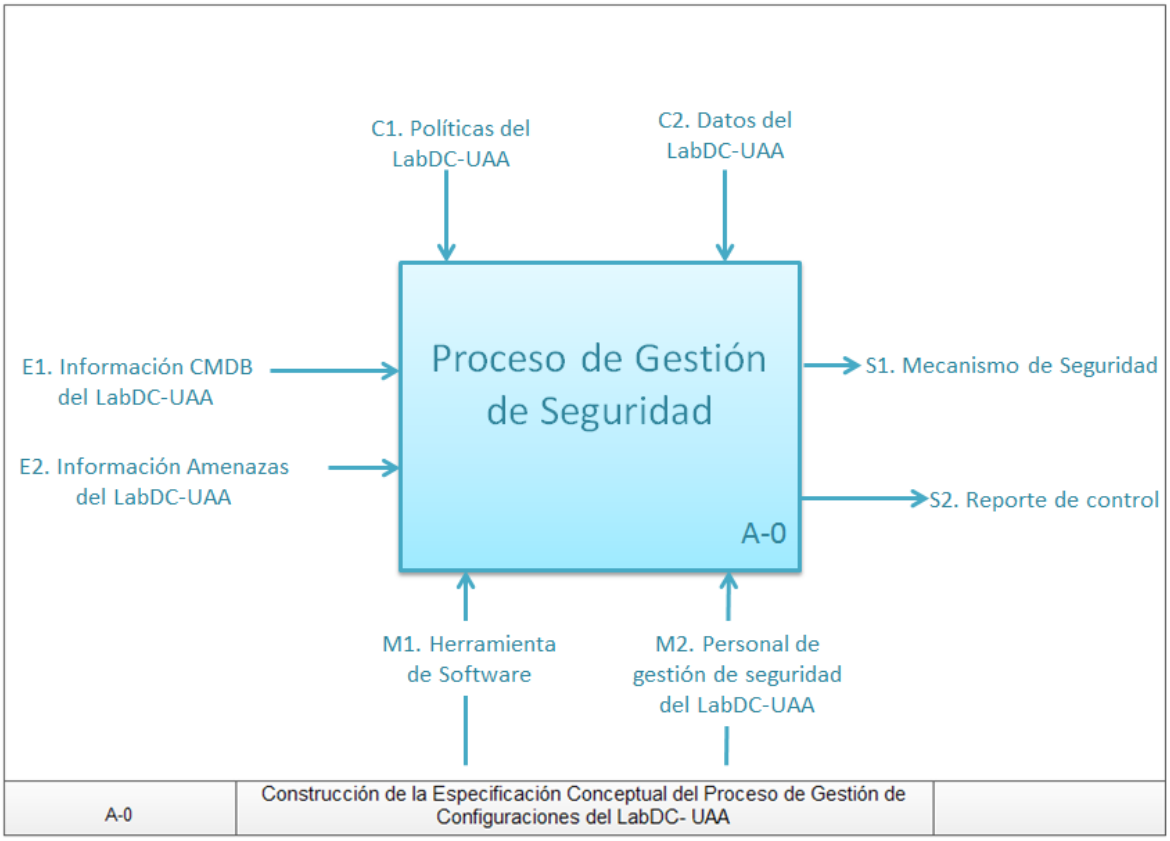


Figura 28 Diagrama IDEF0: Alto Nivel, Caso LabDC-UAA

6.2 Diagrama IDEF0 de Primer Nivel del Proceso de Gestión de Seguridad: Caso LabDC-UAA

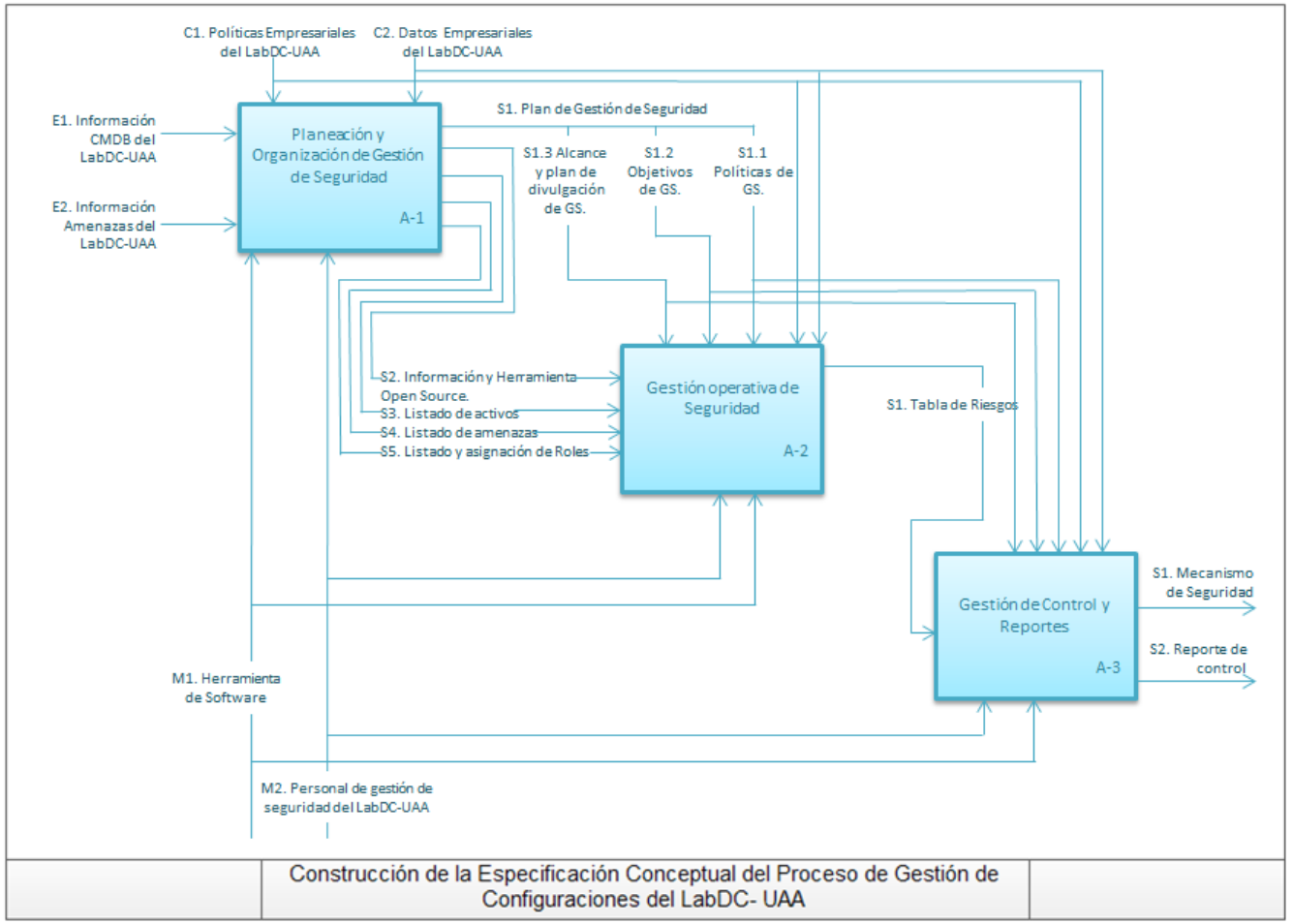


Figura 29 Diagrama IDEF0: Primer Nivel de destalle, Caso LabDC-UAA

6.3 Esquema IDEF0 Detallado del Proceso A-1. Planeación y Organización de Gestión de Seguridad: Caso LabDC-UAA

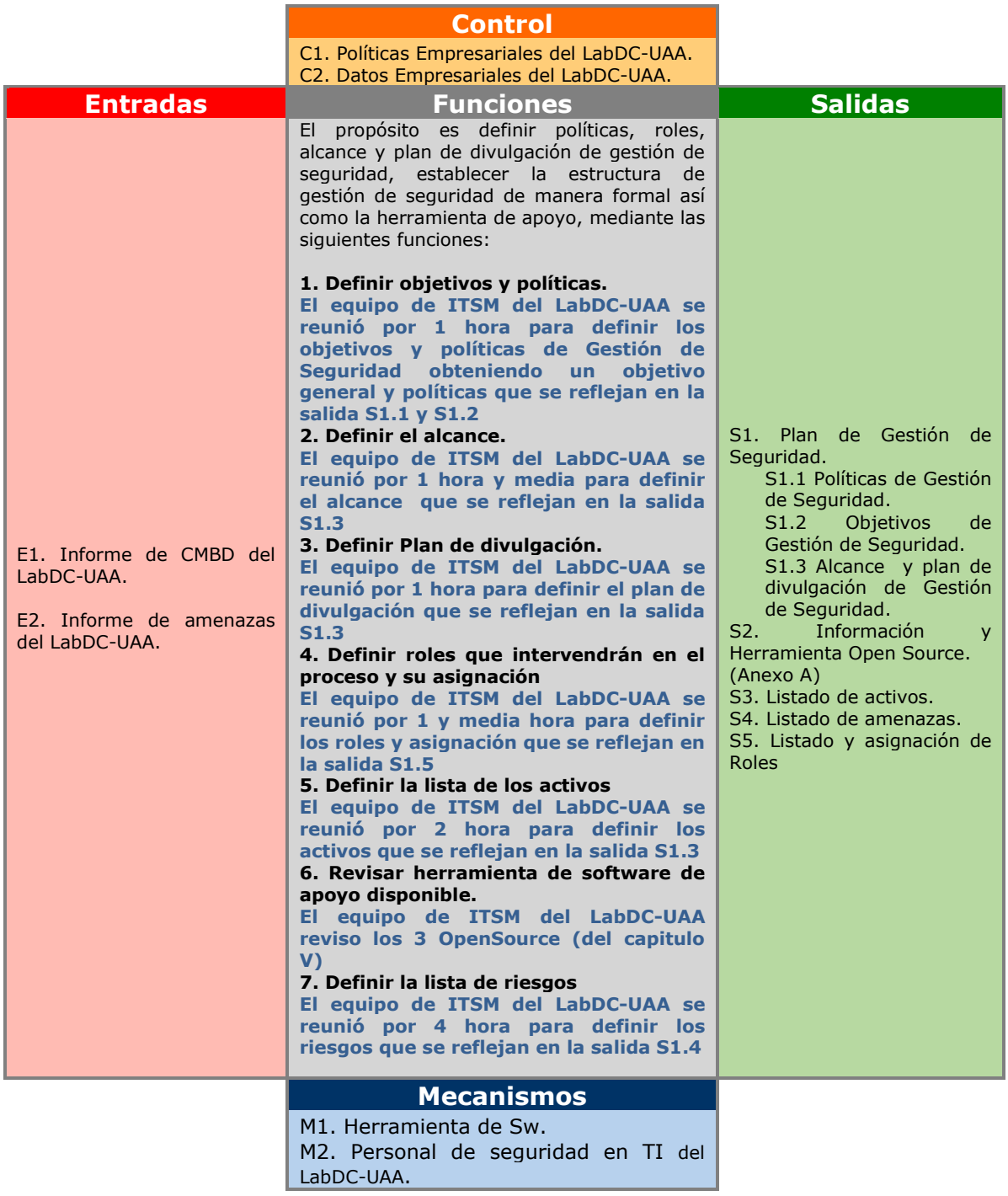


Tabla 12 Salida S1.2 Objetivo: LabDc-UAA

Objetivo general	Implementar un proyecto piloto del proceso de gestión de seguridad apoyado por una herramienta de software open source para el data center de LabDC-UAA.

Tabla 13 Salida S1.1 Politicas: LabDC-UAA

Políticas	1) El proceso de Gestión de la Seguridad hará un seguimiento y gestión de los riesgos para proporcionar un servicio de TI. 2) Cada activo debe tener un responsable de mantener la información exacta y actualizada sobre los efectos de los riesgos posibles que lo afecten. 3) Cada riesgo será identificable y actualizado. 4) Cada activo fundamental o de costo elevado deberá de contar con su análisis de riesgos. 5) Al menos cada semestre se deberá llevar a cabo una auditoría de riesgos registrados en la herramienta de software.

Tabla 14 Salida S1.3 Alcance y plan de divulgación de Gestión de Seguridad: LabDC-UAA

Por el momento el alcance de la implementación cubrirá el LabDC-UAA involucrados para prestar los servicios es su catalogo, que es un servicio de diferentes cursos o herramientas que se suministran a LTI y de la MITC cursos cortos sobre diversos temas de utilidad. Es decir, el nivel de seguimiento que se dará será para los componen que alojan el catalogo de servicios ofrecido por el LabDC-UAA. Para la divulgación del proceso de Gestión de seguridad se manejara la capacitación sobre el proceso previamente mencionado de igual forma sobre la herramienta seleccionada a usar dicha capacitación será dada a todos los usuarios relacionados con el proceso.

Tabla 15 Salida S.3 Activos: LabDC-UAA

ID	Tipo	Activo	Valor Económico	Utilidad	Antigüedad
A.1	Software	Sistema Operativo	M	A	M
A.2	"	Virtualizador	M	A	M
A.3	"	Programas de terceros	B	A	M
A.4	Hardware	Server	A	A	M
A.5	"	Site (Salón de Computo)	A	A	N
A.6	"	Redes (Cableados, switch)	M	A	N
A.7	Datos	Contraseñas de acceso y control	B	A	M
A.8	"	Bases de datos	B	A	M
A.9	"	Documentación sobre el server	B	M	M
A.10	Personal	Personal de Limpieza	B	M	M
A.11	"	Personal de TI	M	A	M

Tabla 16 Salida S.4 Amenazas (Primer parte) : LabDC-UAA

ID	Categoría	Fuente de Amenaza	Acciones Dañinas
R.1	Físicos	Terremoto	Terremoto de escala alta provocando derrumbes de estructuras.
R.2	Proveedores	Fallo en electricidad	Fallo por parte del proveedor de electricidad dejando por minutos sin servicio eléctrico
R.3	Personal de TI	Alteración de información	Personal interno esta modificando datos personales, de los servicios ofrecidos (calificaciones de cursos).

Tabla 17 Salida S.5 Listado y asignación de Roles : LabDC-UAA

Rol	Función
Coordinador de Seguridad	Encargado de registrar activos y amenazas y dar mantenimiento de datos a la CMDB.
Responsable del CI	Es el propietario responsable de la calidad de los datos (de activos, amenazas, contramedidas).
Auditor	Encargado de verificar la integridad de la información (de activos, amenazas, contramedidas).

6.4 Esquema IDEF0 Detallado del Proceso A-2. Gestión operativa de Seguridad: Caso LabDC-UAA

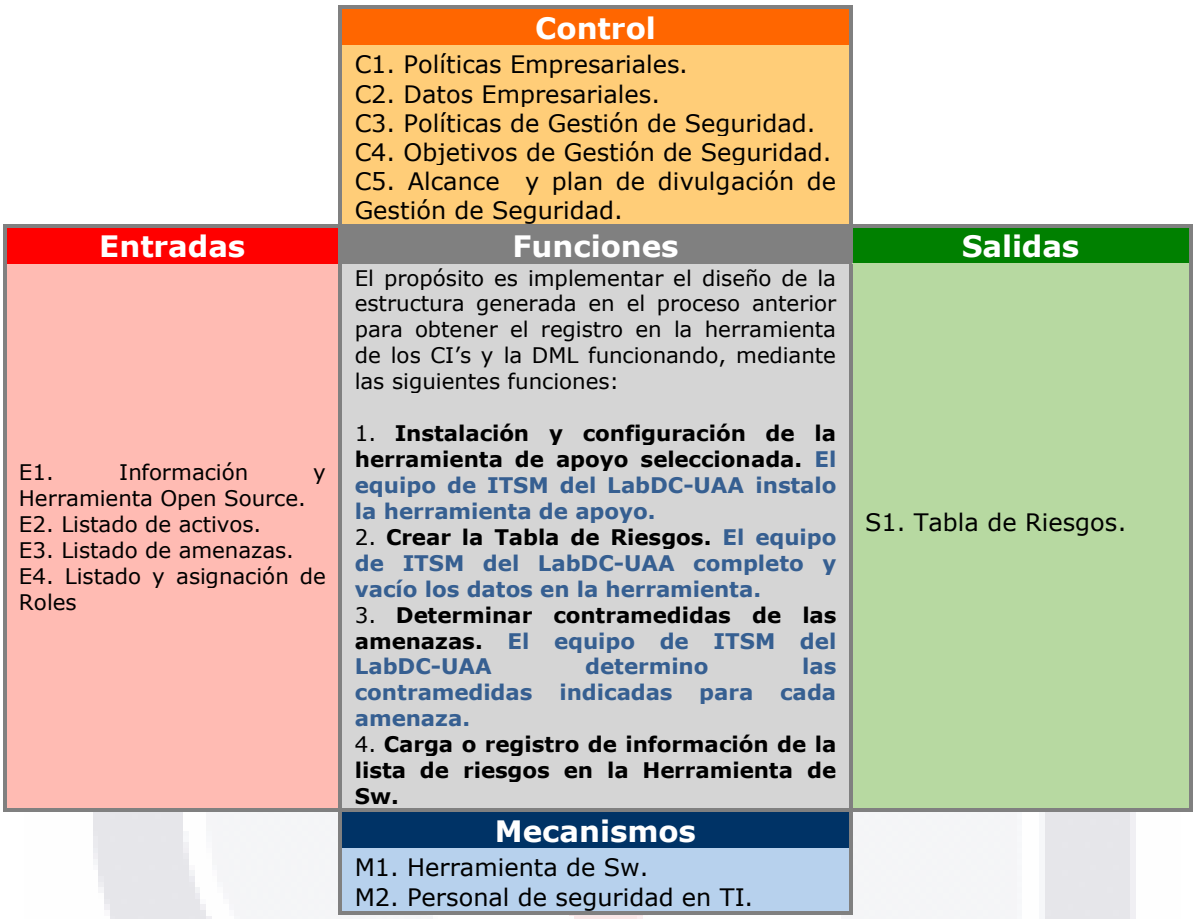


Tabla 18 Salida S.1 Amenazas (Completa) : LabDC-UAA

ID	Categoría	Fuente de Amenaza	Acciones Dañinas	Activos Afectados	Daño	Probabilidad	Exposición al Riesgo
R.1	Físicos	Terremoto	Terremoto de escala alta provocando derrumbes de estructuras.	A.4, A.5, A.6	A	B	A
R.2	Proveedores	Fallo en electricidad	Fallo por parte del proveedor de electricidad dejando por minutos sin servicio eléctrico	A.1, A.3, A.4	B	A	V
R.3	Personal de TI	Alteración de información	Personal interno esta modificando datos personales, de los servicios ofrecidos (calificaciones de cursos).	A.11, A.8	A	M	R

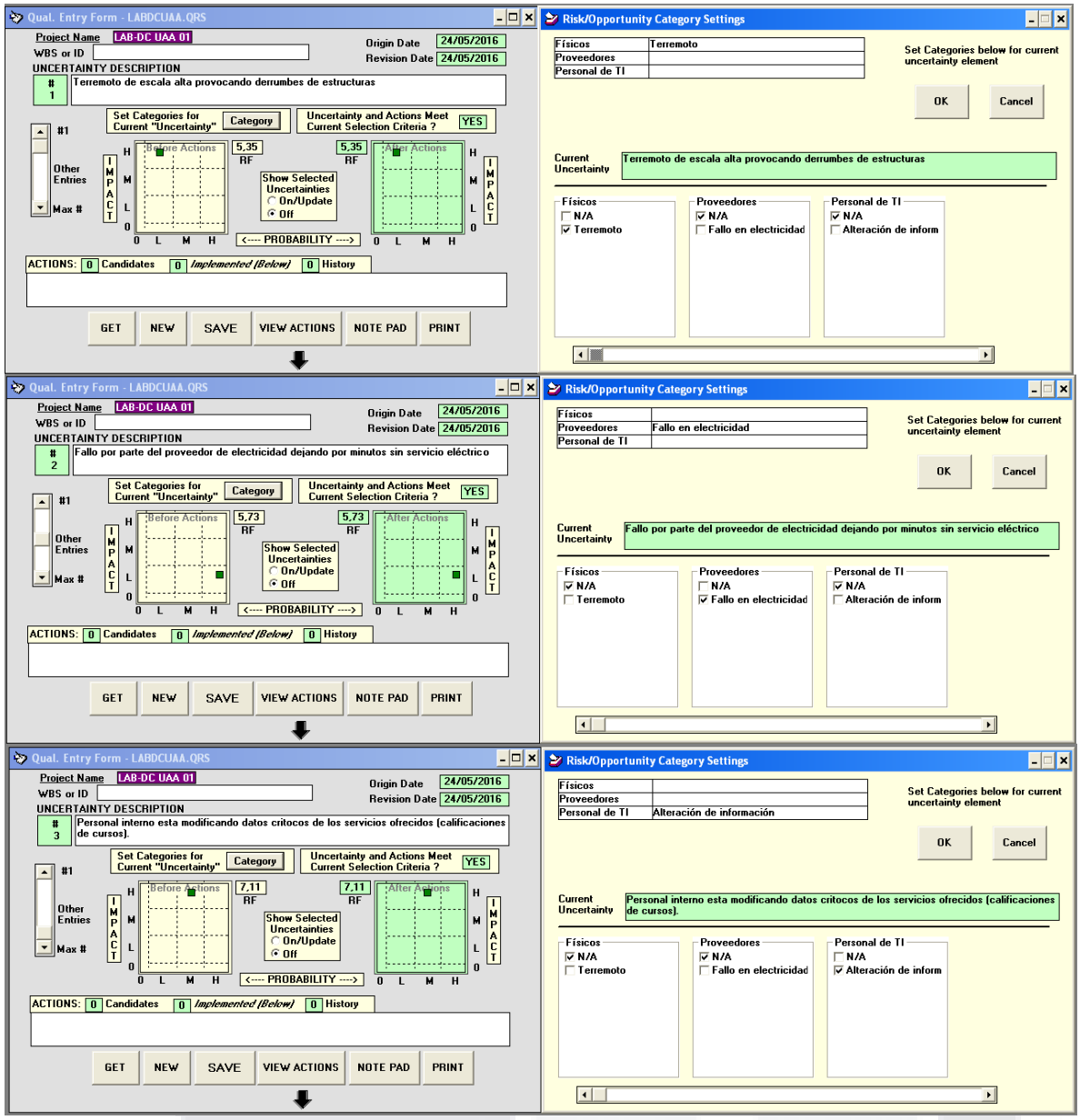


Figura 30 Valores de la Tabla de Riesgos en el Software

Se decide la contramedida para cada uno de las amenazas o posibles riesgos y se recalcula la probabilidad y daño de la amenaza después de la aplicaciones de la contramedida seleccionada:

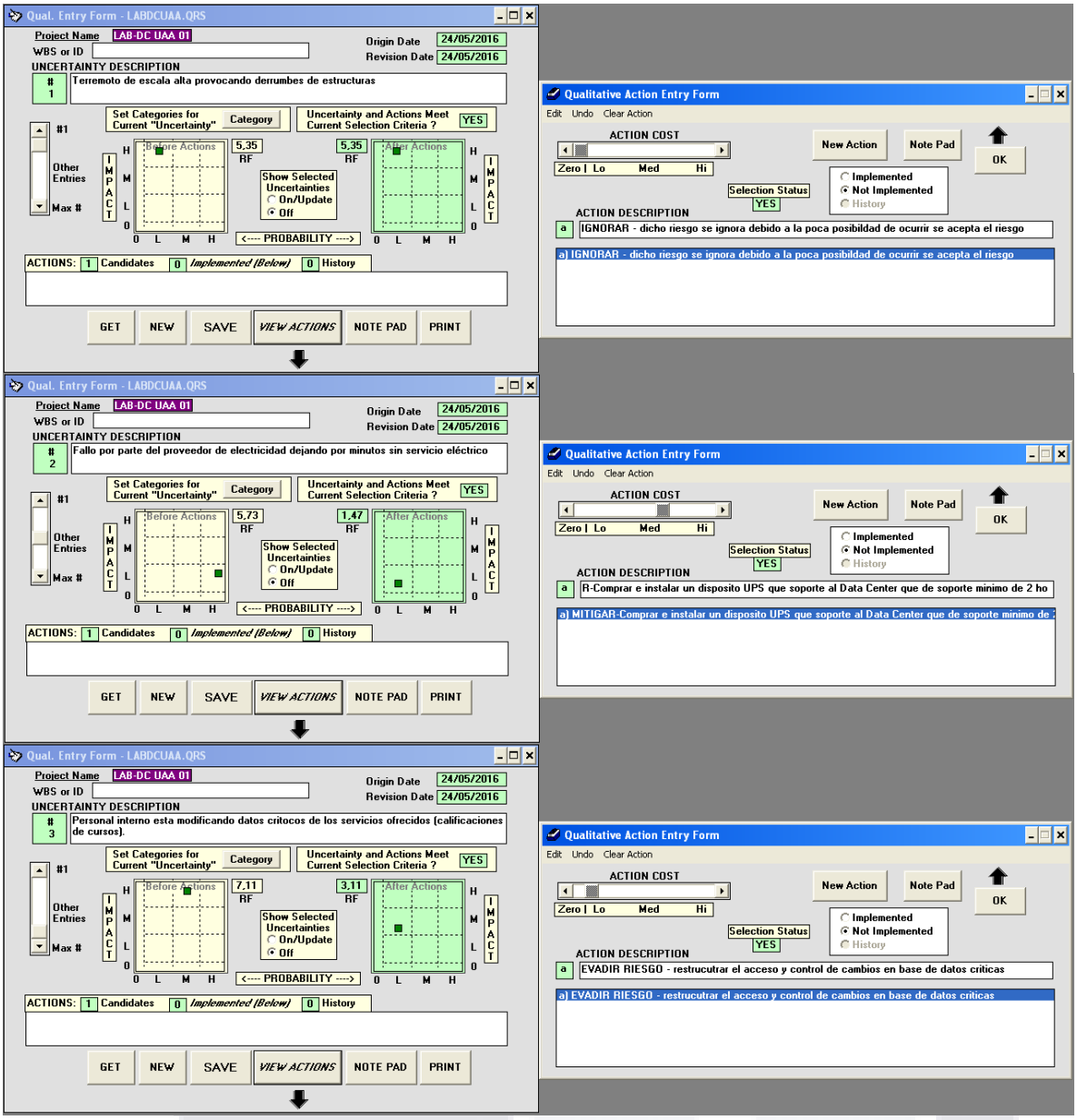
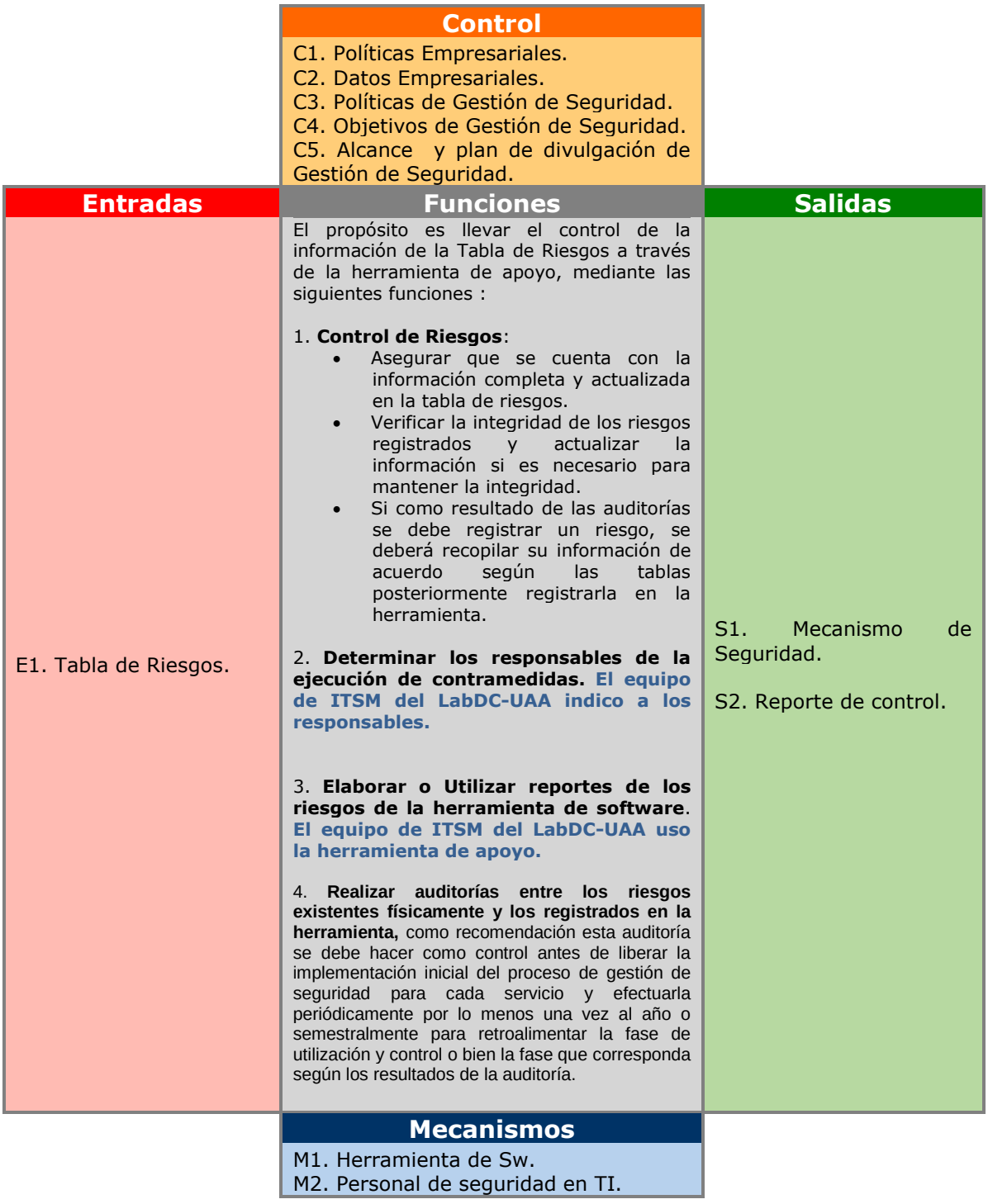


Figura 31 Amenazas y su respectiva contramedida

(con antiguos y nuevos valores de daño y probabilidad según su contramedida)

6.5 Esquema IDEF0 Detallado del Proceso A-2. Gestión de Control y Reportes: Caso LabDC-UAA



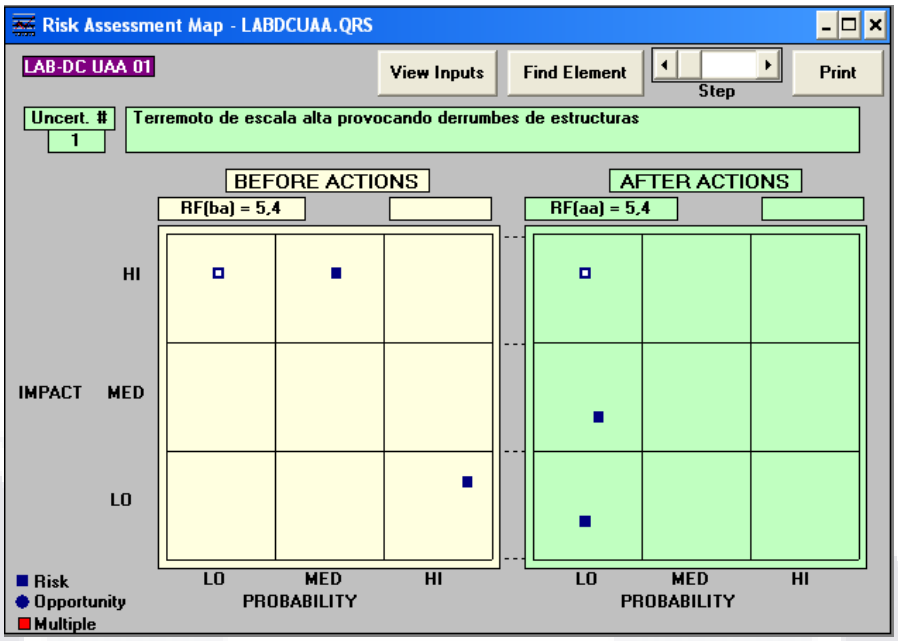


Figura 32 Mapa de Evaluación de Riesgos (con el ejemplo #1)

Figura 33 Mapa para toma de decisiones (Baseline)

Reporte de control

Inicio de Acciones de contramedida: 21-02-2016
Fin de Acciones de contramedida: 16-04-2016

Amenaza ID: R.3

Acciones Dañinas: Personal interno esta modificando datos personales, de los servicios ofrecidos (calificaciones de cursos).

Punto de inicio:
Daño: A
Probabilidad: M
Exposición al Riesgo: R

Contramedida: EVADIR RIESGO – Reestructurar acceso y control en cambios de bases de datos.

Después de aplicación de contramedida:
Daño: M
Probabilidad: B
Exposición al Riesgo: V

Responsable de acción(es): Coordinador de Seguridad

Status de la(s) acción(es): Finalizada

Nombre del auditor: David Montoya (Auditor)
Fecha de revisión: 17-04-2016

Figura 34 Reporte de Control - R.3

VII. Evaluación al proceso de Gestión de Seguridad de servicios de TI usando una herramienta de open source.

Para evaluar el proceso diseñado y aplicado en las secciones anteriores, se utilizan 2 instrumentos de evaluación, los cuales se aplicaron a una muestra piloto de conveniencia, esto es, se aplican a personas profesionistas del área de TI que se tiene acceso y que están familiarizados con el tema por su perfil profesional. Los cuestionarios buscan recopilar datos demográficos y evaluar la metodología a través de los constructos de utilidad, facilidad de uso, compatibilidad, creencias normativas y la actitud final sobre el uso de la metodología. Dichos instrumentos de evaluación se aprecian a continuación:

I.S.C. David Alejandro Montoya Murillo, estudiante de La Maestría en Informática y Tecnologías Computacionales, Universidad Autónoma de Aguascalientes
Dr. José Manuel Mora Tavarez, MC. Jorge E. Macías Luévano, Universidad Autónoma de Aguascalientes, Dr. Jorge Marx Gómez, Universidad de Oldenburg

---

ENCUESTA DEMOGRÁFICA

INSTRUCCIONES. Por favor, antes de llenar el siguiente cuestionario, responda las siguientes preguntas para propósitos demográficos:

---

1 - Marque solamente una respuesta que mejor describa el alcance de las operaciones empresariales de su organización de trabajo:

( ) Regional. ( ) Nacional. ( ) Mundial.

2- Marque solamente una respuesta que mejor describa el nivel de su puesto laboral en su organización:

( ) Una posición técnica de TI en una organización empresarial
( ) Una posición técnica de TI en una Oficina Gubernamental
( ) Un puesto de Gerente den en una organización empresarial
( ) Un puesto de Gerente de TI en una Oficina Gubernamental
( ) Un Académico de TI
( ) Un estudiante de Maestría de tiempo completo

3- Marque solamente una respuesta que mejor describa su máximo nivel escolar alcanzado:

( ) Licenciatura
( ) Especialidad Profesional (después de una Licenciatura)
( ) Graduado de Nivel I (Maestría)
( ) Graduado de Nivel II (Doctorado)

4- Marque solamente una respuesta que mejor describa su rango de edad:
( ) x-24
( ) 25-34
( ) 35-44
( ) 45-54
( ) 55- o más

5.- Marque solamente una respuesta que mejor describa su periodo de tiempo en años utilizando servicios de TI controlados por algún estándar de Gestión de Servicios de TI (ITIL v2, ISO/IEC 20000, MOF 3.0, o CobIT):
( ) 0
( ) 1-3
( ) 4-6
( ) 7-9
( ) 10 o más años

6- Marque solamente una respuesta que mejor describa su situación actual sobre cursos cortos relacionados con cuestiones de Gestión de Servicios de TI que ha tomado:

( ) 0 cursos
( ) 1 - 2 cursos
( ) 3 o más cursos

7.- Marque solamente una respuesta que mejor describa su auto-evaluación actual sobre su experiencia en la comprensión y entendimiento del enfoque de Gestión de Servicios de TI:

( ) Novato (hasta 20%)
( ) Inicial (más de 20% y hasta 40%)
( ) Normal (más de 40% y hasta 60%)
( ) Avanzado (más de 60% y hasta 80%)
( ) Experto (más de 80%)

¡Muchas gracias por su valiosa participación!

I.S.C. David Alejandro Montoya Murillo, estudiante de La Maestría en Informática y Tecnologías Computacionales, Universidad Autónoma de Aguascalientes
Dr. José Manuel Mora Tavarez, MC. Jorge E. Macías Luévano, Universidad Autónoma de Aguascalientes, Dr. Jorge Marx Gómez, Universidad de Oldenburg

---

INSTRUMENTO CONCEPTUAL DE MÉTRICAS DE ACEPTACIÓN DE METODOLOGÍAS.
(Basado en Moore y Benbasat Rara.. Nal.. lene)

INSTRUCCIONES. Favor de asignar de manera personal a cada estatuto el grado de acuerdo o desacuerdo que percibo sobre el **Proceso Simplificado de Gestión de Seguridad basado en ISO 20000, ITIL v2 y MOF v3 para Data Certers Tipo CO-C1 (PS.GesSeg).** en base al Caso Demo análisis y su experiencia en TIs. Para Identificar los Data Centers tipo CO y CI vea la figura 1. Gracias por su colaboración en esto Investigación practica.

Figura 1. Tipos de Data Center y sus Niveles Criticidad (Mora 2013)

Constructo	Total desacuerdo	Desacuerdo	Parcialmente Acuerdo-Desacuerdo	Acuerdo	Total Acuerdo
<Utilidad>	1	2	3	4	5
VR.1 Utilizar la metodología **PS-GesSeg** me habilita a cumplir mis tareos de **Gestión de Seguridad en un Data Center CO-C1 más** rápidamente.					
VR.2 Utilizar la metodología **PS-GesSeg** mejora la calidad de mi **Gestión de Seguridad en un Data Center CO-Cl.**					
VR.3 Usar la metodología **PS-GesSeg** realza la efectividad de mi proceso de **Gestión de Seguridad en un Data Center CO-Cl.**					
VR.4 Usar la metodología **PS-GesSeg** me da mayor control sobre el proceso de **Gestión de Seguridad en un Data Center CO-Cl.**					

Constructo	Total desacuerdo	Desacuerdo	Parcialmente Acuerdo-Desacuerdo	Acuerdo	Total Acuerdo
<facilidad de uso>	1	2	3	4	5
FU.1 Aprender a utilizar/operar la metodología **PS-GesSeg**, sería fácil para mí.					
FU.2 En caso de obligación de usar la metodología **PS-GesSeg**, sería fácil para mí.					
FU.3 En caso de obligación de usar la metodología **PS-GesSeg**, sería difícil para mí.					

Constructo	Total desacuerdo	Desacuerdo	Parcialmente Acuerdo-Desacuerdo	Acuerdo	Total Acuerdo
<compatibilidad>	1	2	3	4	5
CO.1 Utilizar la metodología **PS-GesSeg** para realizar la **Gestión de Seguridad en un Data Center CO-Cl** es compatible culturalmente con todos los aspectos de mi trabajo.					
CO.2 Utilizar la metodología **PS-GesSeg** para realizar la **Gestión de Seguridad en un Data Center CO-Cl** encaja con mi estilo de trabajo.					
CO.3 Utiliza la metodología **PS-GesSeg** para realizar la **Gestión de Seguridad en un Data Center CO-Cl** encaja muy bien con la manera que me gusta gestionar sistemas.					

Constructo	Total desacuerdo	Desacuerdo	Parcialmente Acuerdo-Desacuerdo	Acuerdo	Total Acuerdo
< creencias normativas>	1	2	3	4	5
CN.1 En mi organización de trabajo. la Alta Dirección piensa que se deberían usar metodologías para realizar la **Gestión de Seguridad en un Data Center CO-Cl.**					
CN.2 En mi organización de trabajo, mi director de Informática piensa que se deberían usar metodologías para la **Gestión de Seguridad en un Data Center CO-Cl.**					

CN.3 En mi organización de trabajo, mis colegas desarrolladores piensan que se deberían usar metodologías para realizar la **Gestión de Seguridad en un Data Center CO-Cl.**					
CN.4 En mi contexto cultural de Informática, mis colegas desarrolladores piensan que se deberían usar metodologías para realizar la **Gestión de Seguridad en un Data Center CO-Cl.**					

Constructo < actitud final>	-3	-2	-1	0	1	2	3
AC.1 Después de consideras todo, los aspectos de usar metodologías para realizar **Gestión de Seguridad en un Data Center CO-Cl.** la decisión de usarla en el próximo proyecto es:	Extremadamente Negativo						Extremadamente Positivo
	Extremadamente Desfavorable						Extremadamente Favorable
	Extremadamente Dañino						Extremadamente Benéfico

VIII. Discusión de resultados

Para la evaluación de la metodología diseñada y propuesta para el proceso de gestión de seguridad de TI, se empleó el caso demo del LabDC-UAA, así mismo se brindó un soporte mayor al caso demo con un video demostrativo sobre el uso de la herramienta open source de apoyo seleccionada (PROAct), obteniendo los resultados que se presentan en los siguientes apartados.

8.1 Datos demográficos

Constructo		Porcentaje (%)	Cantidad Absoluta
C1. Alcance de las operaciones empresariales de su organización de trabajo	Regional	0.00	0
	Nacional	80.00	8
	Mundial	20.00	2
C2. Nivel de puesto laboral en su organización	Posición técnica de TI en una organización empresarial	20.00	2
	Posición técnica de TI en una Oficina Gubernamental	50.00	5
	Puesto de Gerente de TI en una organización empresarial	20.00	2
	Puesto de Gerente de TI en una Oficina Gubernamental	10.00	1
	Académico de TI	0.00	0
	Estudiante de Maestría de tiempo completo	0.00	0
C3. Máximo nivel escolar alcanzado	Licenciatura	40.00	4
	Especialidad Profesional (después de una Licenciatura)	0.0	0
	Graduado de Nivel I (Maestría)	50.00	5
	Graduado de Nivel II (Doctorado)	10.00	1

C4. Rango Edad	x-24	0.00	0
	25-34	50.00	5
	35-44	30.00	3
	45-54	10.00	1
	55 - o más	10.00	1
C5. Periodo de tiempo en años utilizando servicios de TI controlados por algún estándar de Gestión de Servicios de TI (ITIL v2, ISO/IEC 20000, ITIL v3, MOF 4.0, o CobIT)	0	10.00	1
	1 - 3	50.00	5
	4 – 6	20.00	2
	7 - 9	10.00	1
	10 – o más	10.00	1
C6. Situación actual sobre cursos cortos relacionados con cuestiones de Gestión de Servicios de TI que ha tomado.	0 cursos	0.00	0
	1 - 2 cursos	70.00	7
	3 - más cursos	30.00	3
C7. Auto-evaluación actual sobre su experiencia en la comprensión y entendimiento del enfoque de Gestión de Servicios de TI	Novato (hasta 20%)	0.00	0
	Inicial (más de 20% y hasta 40%)	20.00	2
	Normal (más de 40% y hasta 60%)	40.00	4
	Avanzado (más de 60% y hasta 80%)	40.00	4
	Experto (más de 80%)	0.00	0

8.2 Evaluación de la Metodología

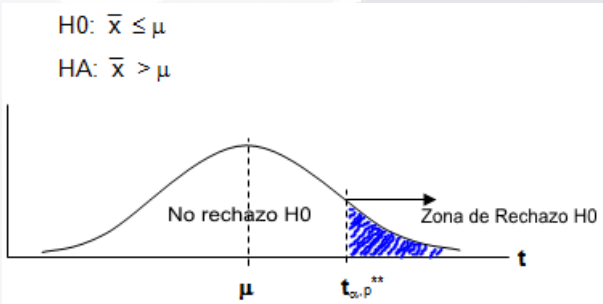
Constructo	Escala	Media	Desviación Estándar
C1. Utilidad	**1..5**	**4.3**	**1.00**
VR.1 Utilizar la metodología PS-GesSeg me habilita a cumplir mis tareas de Gestión de Seguridad en un Data Center CO-C1 más rápidamente.	1..5	4	1.05
VR.2 Utilizar la metodología PS-GesSeg mejora la calidad de mi Gestión de Seguridad en un Data Center CO-Cl.	1..5	4.1	0.88
VR.3 Usar la metodología PS-GesSeg realza la efectividad de mi proceso de Gestión de Seguridad en un Data Center CO-Cl.	1..5	4.1	1.10
VR.4 Usar la metodología PS-GesSeg me da mayor control sobre el proceso de Gestión de Seguridad en un Data Center CO-Cl.	1..5	3.9	1.10
C2. facilidad de uso	**1..5**	**3.77**	**1.38**
FU.1 Aprender a utilizar/operar la metodología PS-GesSeg, seria fácil para mí.	1..5	4.2	1.14
FU.2 En caso de obligación de usar la metodología PS-GesSeg, seria fácil para mí.	1..5	4	1.05
FU.3 En caso de obligación de usar la metodología PS-GesSeg, seria difícil para mí.	1..5	3.1	1.73
C3. Compatibilidad	**1..5**	**3.93**	**1.11**
CO.1 Utilizar la metodología PS-GesSeg para realizar la Gestión de Seguridad en un Data Center CO-Cl es compatible culturalmente con todos los aspectos de mi trabajo.	1..5	3.9	1.10
CO.2 Utilizar la metodología PS-GesSeg para realizar la Gestión de Seguridad en un Data Center CO-Cl encaja con mi estilo de trabajo.	1..5	3.9	1.29
CO.3 Utiliza la metodología PS-GesSeg para realizar la Gestión de Seguridad en un Data Center CO-Cl encaja muy bien con la manera que me gusta gestionar sistemas.	1..5	4	1.05

C4. Creencias Normativas	**1..5**	**3.95**	**1.15**
CN.1 En mi organización de trabajo, la Alta Dirección piensa que se deberían usar metodologías para realizar la Gestión de Seguridad en un Data Center CO-Cl.	1..5	3.9	1.45
CN.2 En mi organización de trabajo, mi director de Informática piensa que se deberían usar metodologías para la Gestión de Seguridad en un Data Center CO-Cl.	1..5	4.2	1.14
CN.3 En mi organización de trabajo, mis colegas desarrolladores piensan que se deberían usar metodologías para realizar la Gestión de Seguridad en un Data Center CO-Cl.	1..5	3.8	1.03
CN.4 En mi contexto cultural de Informática, mis colegas desarrolladores piensan que se deberían usar metodologías para realizar la Gestión de Seguridad en un Data Center CO-Cl.	1..5	3.9	1.10
C5. Actitud Final	**-3..3**	**1.43**	**0.94**
AC.1 Después de consideras todo, los aspectos de usar metodologías para realizar Gestión de Seguridad en un Data Center CO-Cl. la decisión de usarla en el próximo proyecto es: Extremadamente Negativo ... Extremadamente Positivo	-3..3	1.5	0.85
Extremadamente Desfavorable ... Extremadamente Favorable	-3..3	1.5	0.85
Extremadamente Dañino ... Extremadamente Benéfico	-3..3	1.3	1.16

8.3 Análisis estadísticos

Para realizar el análisis estadístico se hará un análisis de medias y debido a que se tienen pocas muestras (n<30), se empleará una distribución t-student de un solo extremo para cada constructo a fin de obtener conclusiones de las evaluaciones obtenidas.

Gráficamente la prueba t – student de un extremo se interpreta de la siguiente manera:



Para obtener los valores de t□, □ se utilizó la tabla de distribución t que se incluye en el anexo, y los cálculos se realizaron en Microsoft Excel 2010.

8.3.1 Constructo 1: Utilidad

HIPÓTESIS:

H0 utilidad**:** $\bar{X}$ utilidad □$\leq$ 3.0

HA utilidad: $\bar{X}$ utilidad > 3.0

Al aplicar la prueba t de un solo extremo se obtuvieron los siguientes datos:

Media ($\bar{X}$)	Desviación estándar (S)	N	t	μ	α (n-1)	p	t**
4.03	1.00	**10**	**3.24**	3	9	0.05	**1.83**

Por lo tanto, como t > t** entonces podemos rechazar H0 a un nivel de significancia del 5%. Es decir, la gente percibe como muy útil la metodología propuesta para implementar el proceso de gestión de seguridad en el área de TI de sus organizaciones.

8.3.2 Constructo 2: Facilidad de Uso

HIPÓTESIS:

$$\mathbf{H0}_{\text{facilidadUso}}: \bar{X}_{\text{facilidadUso}} \leq 3.0$$

$$\mathbf{HA}_{\text{facilidadUso}}: \bar{X}_{\text{facilidadUso}} > 3.0$$

Al aplicar la prueba t de un solo extremo se obtuvieron los siguientes datos:

Media ($\bar{X}$)	Desviación estándar (S)	N	t	μ	α (n-1)	p	t**
3.77	1.38	**10**	**1.75**	3	9	0.05	**1.83**

Por lo tanto, como t < t** entonces NO podemos rechazar H0 a un nivel de significancia del 5%. Esto es que la metodología se percibe como No Fácil de usar por lo que se observa que es necesario un periodo de entrenamiento para poder emplearla para implementar el proceso de gestión de seguridad.

8.3.3 Constructo 3: Compatibilidad

HIPÓTESIS:

$$\mathbf{H0}_{\text{compatibilidad}}: \bar{X}_{\text{compatibilidad}} \leq 3.0$$

$$\mathbf{HA}_{\text{compatibilidad}}: \bar{X}_{\text{compatibilidad}} > 3.0$$

Al aplicar la prueba t de un solo extremo se obtuvieron los siguientes datos:

Media ($\bar{X}$)	Desviación estándar (S)	N	t	μ	α (n-1)	p	t**
3.93	1.11	**10**	**2.65**	3	9	0.05	**1.83**

Por lo tanto, como t > t** entonces podemos rechazar H0 a un nivel de significancia del 5%. Es decir, la metodología propuesta es percibida por las personas como adecuadamente compatible con su cultura empresarial y con su forma de trabajar en el área de TI de sus organizaciones.

8.3.4 Constructo 4: Creencias Normativas

HIPÓTESIS:

$$\mathbf{H0}_{\text{creenciasNormativas}}: \bar{X}_{\text{creenciasNormativas}} \leq 3.0$$

$$\mathbf{HA}_{\text{creenciasNormativas}}: \bar{X}_{\text{creenciasNormativas}} > 3.0$$

Al aplicar la prueba t de un solo extremo se obtuvieron los siguientes datos:

Media ($\bar{X}$)	Desviación estándar (S)	N	t	μ	α (n-1)	p	t**
3.95	1.15	**10**	**2.60**	3	9	0.05	**1.83**

Por lo tanto, como t > t** entonces podemos rechazar H0 a un nivel de significancia del 5%. Esto es que la metodología propuesta se percibe por las personas del área de TI en las organizaciones como una metodología que se debería usar para realizar el proceso de gestión de seguridad.

8.3.5 Constructo 5: Actitud Final

HIPÓTESIS:

$$\mathbf{H0}_{\text{actitudFinal}}: \bar{X}_{\text{actitudFinal}} \leq 3.0$$

$$\mathbf{HA}_{\text{actitudFinal}}: \bar{X}_{\text{actitudFinal}} > 3.0$$

Al aplicar la prueba t de un solo extremo se obtuvieron los siguientes datos:

Media ($\bar{X}$)	Desviación estándar (S)	N	t	μ	α (n-1)	p	t**
1.43	0.94	**10**	**4.85**	0	9	0.05	**1.83**

Por lo tanto, como t > t** entonces podemos rechazar H0 a un nivel de significancia del 5%. Es decir que las personas perciben como positivo, benéfico y favorable el uso de la metodología propuesta en su próximo proyecto, lo que indica un gran interés en utilizarla para implementar el proceso de gestión de seguridad de TI en proyectos futuros.

Conclusión

Conclusiones de las Hipótesis:

H1. La Fase de Procesos de Control de ISO 20000 efectivamente tiene procesos para ser usados en un Diseño de un proceso de gestión de TI y existe correspondencia con procesos en ITIL v2 y MOF v3.

H2.- Fue posible diseñar un Proceso de gestión de seguridad de servicios de TI basado en ISO 20000 y complementado con los sub-procesos asociados de ITIL v2 e MOF v3.

H3. El Proceso diseñado se logro que estuviera apoyado con una herramienta open source.

H4. Los valores obtenidos en los constructos de UTILIDAD, FACILIDAD DE USO, COMPATIBILIDAD, CREENCIAS NORMATIVAS Y ACTITUD FINAL percibidos por una muestra piloto de Profesionistas en TI de Data Centers similares al LabDC-UAA al evaluar el Modelo diseñado y la Herramienta de Soporte resultaron adecuados, tan solo se distingue que será recomendable optar por la capacitación sobre el Modelo y la herramienta.

Al concluir la revisión de los marcos de gestión de servicios (ITIL v2, MOF v3 e ISO 20000) y desde mi propio punto de vista creo que en la actualidad es necesario el ajuste de estas metodologías a lo que es la "realidad" de las organizaciones en México, ya que por ser tan extensas y detalladas, así como de requerir de una alta inversión de recursos (tanto en tiempo, recursos humanos y sobre todo financieros), se vuelve compleja la adopción de estándares como ITIL e ISO 20000 para la gestión de servicios de TI, ya que el costo beneficio es a largo plazo, situación que no es muy conveniente al área de enfoque en la que centramos el proceso. En base a esto, y dada la importancia, de acuerdo a la literatura revisada del proceso de gestión de

seguridad, para la gestión de recursos y garantizar una mejor calidad en los servicios, se puede concluir que la metodología desarrollada en este trabajo es un importante aporte ya que el diseño incluye los puntos clave o básicos minimos requeridos para la implementación del proceso de gestión de seguridad, además de brindar la opción del uso de la herramienta de apoyo Open Source para soportar dicho proceso cuidando no afectar la salud financiera de la organización que lo decida implantar.

A través del análisis de las evaluaciones obtenidas para la metodología propuesta se puede concluir lo siguiente:
La metodología propuesta en este trabajo para la implementación del proceso de gestión de seguridad con apoyo de la herramienta open source seleccionada (PROAct), es percibida por las personas como bastante útil, compatible con su forma y necesidades de trabajo y que va de acuerdo con los principios y conductas de trabajo de sus organizaciones. Sin embargo, también se puede percibir que en cuanto a la facilidad de uso se requiere de un periodo de entrenamiento/capacitación para poder emplearlo correctamente tanto en el seguimiento del proceso o como el uso de la herramienta. Y finalmente las personas perciben como positivo, benéfico y favorable el uso de la metodología propuesta en su próximo proyecto, lo que indica un gran interés en utilizarla para implementar el proceso de gestión de seguridad de TI en proyectos futuros.

Definitivamente el uso de metodologías formales permite optimizar de forma efectiva los servicios de TI dentro de una organización chica, mediana o grande. Se ha demostrado que toda implementación de ITIL ha permitido hacer más efectivos los servicios de informática, los de producción y administrativos en todos los aspectos clave para el crecimiento organizacional. Por lo que trabajos de investigación como este deben ser tomados en cuenta por las áreas de Tecnologías de Información de las organizaciones para mejorar y/o reinventar su forma de trabajo incluyendo sus procesos e infraestructura, que pueden aportar ventajas competitivas al tener bien definido por donde empezar y que

hacer primero así como claramente definidos sus procesos y tareas a seguir donde ya está sintetizado y adaptado el contenido de estándares tan extensos y complejos como ITIL y MOF o tan abstractos como ISO 20000.

Esta tesis, por tanto, contribuye al avance del proceso de gestión de Laboratorios de Data Center para organizaciones de tamaño pequeño o mediano, donde los altos costos impedían la adquisición de herramientas ITSM comerciales y la contratación de costosos consultores ITSM, a través de la provisión de un proceso esencial apoyado por una herramienta open source.

Aunque el diseño propuesto cuenta con ciertas limitaciones como:

- Se usaron los estándares y documentos en sus versiones disponibles proporcionados por el Director de Tesis.
- El levantamiento de datos sobre el caso de estudio fue limitado, ya que se requería que cumplieran con un cierto perfil: Conocimiento de metodologías de Gestión de servicios, encontrarse en áreas de TI y tener experiencia en el uso del enfoque de gestión de servicios, así como un cierto nivel de experiencia en el área de gestión de seguridad.
- La investigación se realizó con una Especificación y Validación Conceptual del Proceso de Gestión de Seguridad aplicándolo a un caso de prueba prototipo para un Data Center en el sector educativo. Específicamente para un servicio ofrecido en el Laboratorio Data Center de la UAA del Departamento de Sistemas de Electrónicos. Aunque el proceso se diseñó de manera genérica y puede ser usado de manera general pudiera requerir de algún ajuste.
- Las herramientas propuestas al ser open source tienen ciertas limitantes, hablando específicamente de PROAct por ejemplo no permite generar mas de 10 entidades, otra es que la herramienta no esta traducida al español, ya que el idioma ingles es el idioma de origen del PROAct.

En relación a trabajos futuros relacionados o basados en este, se puede distinguir en el resultado de la investigación en que los trabajadores de TI en las organizaciones ven como una aportación clara el uso de estándares no tan

complejos y posibles de adecuar a su modo de trabajo y tecnologías. De igual forma la aceptación de un proceso apoyado por una herramienta para la gestión de seguridad.

Glosario

Activo: Es cualquier capacidad, recurso o ambos, dependiendo del contexto, incluye todo lo que pueda contribuir a la prestación de un servicio, pueden ser desde una gestión, organización, proceso, conocimiento, personas, información, aplicaciones, infraestructura y capital financiero.

Alcance: Es el limite o grado en que se aplica un proceso, procedimiento, certificación, contrato, etc.

Amenaza: es una fuente causante o co-generadora de riesgos.

Auditoria: Inspección formal para verificar si se está siguiendo/cumpliendo un estándar o un conjunto de guias, que sus registros son precisos o que las metas de eficiencia y efectividad se están cumpliendo. Una auditoria la puede realizar tanto un grupo interno como uno externo.

Cambio: Adición, modificación o eliminación de algo que podría afectar a los servicios de TI.

Calidad: Es la capacidad de un producto, servicio o proceso para proporcionar el valor previsto. Por ejemplo, un componente de hardware puede ser considerado como de alta calidad si tiene el desempeño que se espera y proporciona la confiabilidad requerida.

CI (Elemento de Configuración): Puede ser hardware de una computadora, todo tipo de software, componentes de red, servidores, procesadores, documentación, procedimientos, servicios, licencias de uso, entre otros componentes de TI que deban ser controlados por la organización.

CMDB (Base de Datos de Gestión de Configuraciones): Base de datos usada para almacenar registros de configuración durante todo su ciclo de vida. La CMDB contiene atributos de CI's, y relaciones con otros CI's.

COBIT: Objetivos de Control para la Información y Tecnologías Relacionadas (COBIT) proporciona orientación y las mejores practicas para la gestión de procesos de TI. COBIT es publicado por ISACA, en conjunto con el Instituto de Gobierno de TI (IT Governance Institute - ITGI).

DHL (Biblioteca Definitiva de Hardware): En ITIL v2 se plantea, dentro del proceso de gestión de configuraciones, la creación de un lugar donde se deberán almacenar elementos de Hardware de respaldo.

DML (Biblioteca definitiva de Medios): En ITIL v3 es uno o más lugares en los que las versiones definitivas y autorizadas de todos los elementos de configuración de software se almacenan en forma segura. Puede contener licencias y documentación. La biblioteca definitiva de medios está controlada por la gestión de activos de servicio.

DSL (Biblioteca definitiva de Software): En ITIL v2 se plantea, dentro del proceso de gestión de configuraciones, la creación de un lugar donde se deberán almacenar copia de las versiones finales del software que se encuentra en el ambiente de producción.

Gestión de activos de servicio y configuración (SACM): En ITIL v3, es el proceso responsable de asegurar que los activos, requeridos para entregar servicios, están debidamente controlados, y que haya información precisa y confiable sobre esos activos y que esté disponible cuando y donde se necesite. Esta información incluye detalles de como se han configurado los activos y las relaciones entre ellos.

Gestión de Incidentes: Proceso responsable de la gestión del ciclo de vida de todos los incidentes. La gestión de incidentes asegura que se restablezca la operación normal de servicio lo antes posible y se minimice el impacto al negocio.

Gestión de Problemas: Es el proceso responsable de la gestión del ciclo de vida de todos los problemas. La gestión de problemas previene proactivamente la ocurrencia de incidentes y minimiza el impacto de los incidentes que no se pueden prevenir.

Infraestructura de TI: Es todo el hardware, software, redes, instalaciones, etc., que se necesitan para desarrollar, probar, entregar, monitorear, controlar o dar soporte a servicios de TI y a aplicaciones. El termino incluye toda la tecnología de información, pero no a las personas, procesos y ni documentación asociadas.

ISO 20000: Es un marco de administración de servicios de TI. Esta norma promueve la adopción de un enfoque de procesos integrados, para una provisión eficaz de servicios gestionados que satisfaga los requisitos del negocio y de los clientes.

ITIL: Biblioteca de Infraestructura de Tecnologías de Información. Es un conjunto de publicaciones de mejores practicas para la gestión de servicios que han usado con éxito grandes organizaciones. ITIL proporciona guias de calidad para la prestación de servicios de TI y los procesos, las funciones y otras competencias necesarios para sustentarlas.

ITIL v2: El marco de trabajo ITIL se basa en el ciclo de vida de servicio y dicho ciclo consta de dos partes: 1) Liberación del servicio (que incluye los procesos: gestión del nivel del servicio, gestión financiera de TI, gestión de disponibilidad, gestión de capacidad, gestión de continuidad de servicio de TI) y 2) Soporte del servicio (que incluye los procesos: Función de mesa de servicio, gestión de incidentes, gestión de problemas, gestión de cambios, gestión de configuraciones y gestión de lanzamientos)

ITIL v3: El marco de trabajo ITIL se basa en el ciclo de vida de servicio y dicho ciclo consta de cinco etapas (estrategia del servicio, diseño del servicio, transición del servicio, operación del servicio y mejora continua del servicio).

ITSM (Gestión de Servicios de TI): de sus siglas en ingles: IT Service Management. Es la implementación y gestión de la calidad de los servicios de TI que cumplan las necesidades del negocio.

MOF: Microsoft Operations Framework, es un marco de referencia para todos los Administradores de TI, en el que podrán encontrar una serie de guías prácticas para actividades de TI cotidianas y que los ayudará a lo largo de todo el ciclo de vida de TI.

Open Source: El código abierto es el software distribuido y desarrollado libremente es decir sin costo alguno. Se centra más en los beneficios prácticos (acceso al código fuente) que en cuestiones éticas o de libertad que tanto se destacan en el software libre.

Probabilidad de riesgos: es un valor numérico u ordinal (calculado o estimado) de la frecuencia de ocurrencia del riesgo.

Relación: Es una conexión o interacción entre dos personas o cosas. En la gestión de activos de servicio y configuración, es un enlace entre dos elementos de configuración que identifica a una dependencia o conexión entre ellos. Por ejemplo, las aplicaciones pueden estar vinculadas a los servidores en los que se ejecutan y los servicios de TI tienen muchos vínculos con todos los elementos de configuración que contribuyen a ese servicio de TI.

Riesgo: es un evento que puede suceder (donde es posible o no estimar su probabilidad de ocurrencia) con consecuencias negativas (perdida o disminución de un recurso valioso).

RFC (Requerimiento de Cambio): Es una propuesta formal para hacer un cambio. Incluye los detalles del cambio propuesto, y puede ser registrado en papel o electrónicamente.

Rol: Es un conjunto de responsabilidades, actividades y autoridad asignadas a una persona o equipo. Un rol se define en un proceso o función. Una persona o equipo puede tener múltiples roles - por ejemplo, los roles del gerente de configuración y del gerente de cambios puede ser llevados a cabo por una sola persona. La palabra rol también se utiliza para describir el propósito de algo o para qué se utiliza.

Servicio: Medio para proporcionar valor al usuario al facilitar los resultados que desean alcanzar los usuarios sin la necesidad de que asuman los costos y riesgos específicos asociados.

Servicio de TI: Es un servicio proporcionado por un proveedor de servicios de TI. Un servicio de TI se compone de una combinación de tecnología de información, personas y procesos.

TI: Tecnología de Información. Es el uso de la tecnología para el almacenamiento, la comunicación o el procesamiento de la información. Típicamente, la tecnología incluye computadores(as), telecomunicaciones, aplicaciones y otro software. La información puede incluir datos del negocio, voz, imágenes, video, etc.

Bibliografía

- Abimbola, A. (2007). Information security incident response. *Network Security*, *2007*(12), 10–13. http://doi.org/10.1016/S1353-4858(07)70103-4
- Alejandro Fuentes-Penna, Ocotlán Díaz-Parra, José C. Zavala-Díaz, Jorge A. Ruiz-Vanoye, Juan C. Olivares- Rojas, Guideline of Identification and Track on Support's level on Mexican Very Small Enterprises (MVSE), International Journal of Combinatorial Optimization Problems and Informatics, vol. 1, núm. 1, mayo-agosto, 2010, pp. 50-55.
- B. D. Jenkins,. (1998). Risk Analysis helps establish a good security posture; Risk Management keeps it that way. Recuperado el 2 de abril de 2016, a partir de https://www.nr.no/~abie/RA_by_Jenkins.pdf
- Cartlidge, A., & LILLYCROP, M. (2004). An Introductory Overview of ITIL®, Version 1.0. *Published by: The UK Chapter of the it SMF*.
- Cater-Steel, A., & Tan, W.-G. (2005a). Implementation of IT infrastructure library (ITIL) in Australia: progress and success factors. En *2005 IT Governance International Conference* (pp. 39–52). Auckland, New Zealand: Auckland University of Technology. Recuperado a partir de http://eprints.usq.edu.au/998/
- Cater-Steel, A., & Tan, W.-G. (2005b). *itSMF Australia 2005 Conference: Summary of ITIL Adoption Survey Responses* (Report). Toowoomba, Australia: University of Southern Queensland. Recuperado a partir de http://eprints.usq.edu.au/2992/
- Cater-Steel, A., Toleman, M., & Tan, W.-G. (2006). Transforming IT service management - the ITIL impact. En S. Spencer & A. Jenkins (Eds.), *Proceedings of the 17th Australasian Conference on Information Systems (ACIS 2006)*. Australia: Australasian Association for Information Systems. Recuperado a partir de http://www.acis2006.unisa.edu.au/
- Doughty, K. (2003). Implementing enterprise security: a case study. *Computers & Security*, *22*(2), 99–114. http://doi.org/10.1016/S0167-4048(03)00205-0

- Forte, D. (2007). Security standardization in incident management: the ITIL approach. *Network Security*, *2007*(1), 14–16. http://doi.org/10.1016/S1353-4858(07)70007-7
- Fuentes-Penna, A., Díaz-Parra, O., Zavala-Díaz, J. C., Ruiz-Vanoye, J. A., & Olivares-Rojas, J. C. (2010). Guideline of Identification and Track on Support's level on Mexican Very Small Enterprises (MVSE). Recuperado el 4 de diciembre de 2014, a partir de http://www.redalyc.org/resumen.oa?id=265219741006
- Fumy, W. (2004). IT security standardisation. *Network Security*, *2004*(12), 6–11. http://doi.org/10.1016/S1353-4858(04)00169-2
- Galup, S. D., Dattero, R., Quan, J. J., & Conger, S. (2009). An Overview of IT Service Management. *Commun. ACM*, *52*(5), 124–127. http://doi.org/10.1145/1506409.1506439
- Hochstein, A., Tamm, G., & Brenner, W. (2005). Service oriented IT management: benefit, cost and success factors. *ECIS 2005 Proceedings*, 98.
- Inform-IT. (2007). *Foundations of ITIL V3* (1st edition). Zaltbommel, Netherlands: Van Haren Publishing.
- Lucio-Nieto, T., Colomo-Palacios, R., Soto-Acosta, P., Popa, S., & Amescua-Seco, A. (2012). Implementing an IT service information management framework: The case of COTEMAR. *International Journal of Information Management*, *32*(6), 589–594. http://doi.org/10.1016/j.ijinfomgt.2012.08.004
- Potgieter, B. C., Botha, J. H., & Lew, C. (2005). Evidence that use of the ITIL framework is effective. En *18th Annual conference of the national advisory committee on computing qualifications, Tauranga, NZ* (pp. 160–167). Citeseer.
- Talla, M., Valverde, R., Talla, M., & Valverde, R. (2013). An Implementation of ITIL Guidelines for IT Support Process in a Service Organization. *International Journal of Information and Electronics Engineering*, *3*(3), 334–341.

- Ying, L., Lijun, X., & Wei, S. (2009). Key Issues for Implementing Configuration Management. En *The 2009 International Symposium on Web Information Systems and Applications (WISA 2009)* (p. 347). Recuperado a partir de http://academypublisher.com/proc/wisa09/papers/wisa09p347.pdf
- Draft Federal Information Processing Standards: "Announcing the Standard for integration definition for function modeling (IDEF0)". Publication 183, December 21,1993
- Mora, Manuel, Documentos de Diseño del Laboratorio Data Center del Departamento de Sistemas Electrónicos, 2012.
- Mora, Manuel. Notas del curso Taller III, Universidad Autónoma de Aguascalientes, 2013
- Mora Manuel, O'Connor Rory, Raisinghani Mahesh, Gelman Ovsei, ITSDM ITS V01 MANUAL (based on ISO 20000 and ITIL V3), 2013
- http://coras.sourceforge.net/
- http://www.katmarsoftware.com/pra.htm
- http://maxvalue.com/pabroch.htmt

Anexos

Anexo A .- Manual de uso de la herramienta PROAct(caso Cuanlitativo)

Anexo B .- Formato de Reporte de control

Anexo C .- Tabla de la Distribución t

Anexo D .- Servicios en http://148.211.145.149

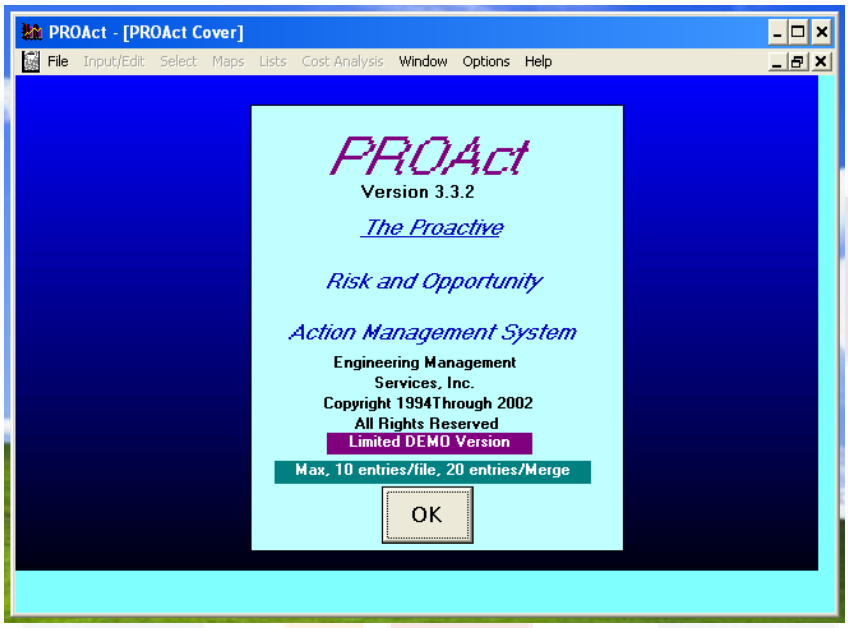
Anexo E .- Video Complemento de la Implementación del Caso LabDC-UAA: Servicio Moodle II

Anexo A .- Manual de uso de la herramienta PROAct(caso Cuanlitativo)

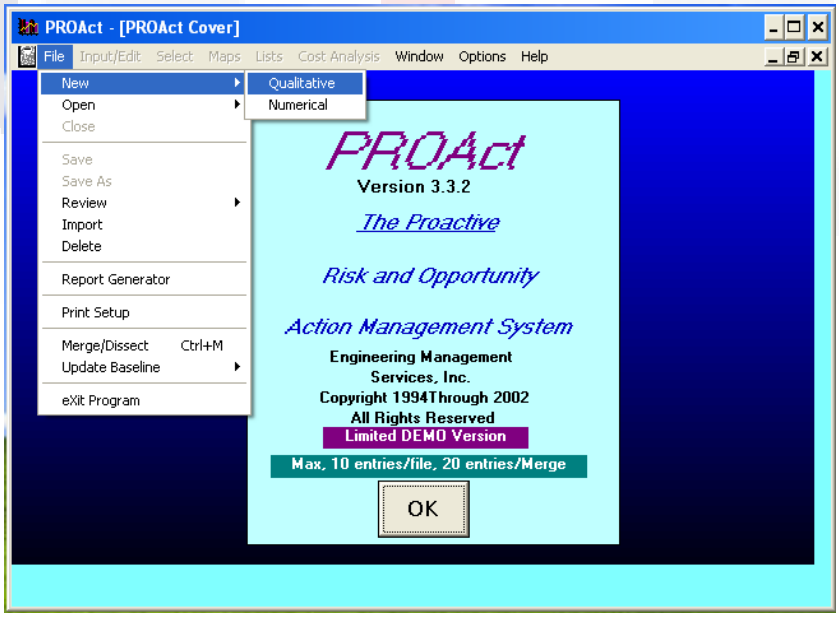
PROAct V3.3.2

1. Inicialización

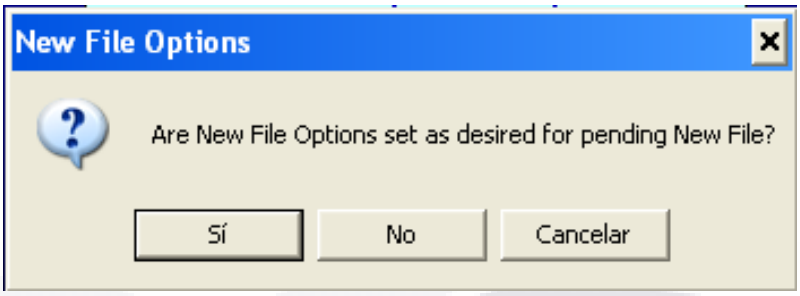
1.1 Ejecutar software demo ProAct.



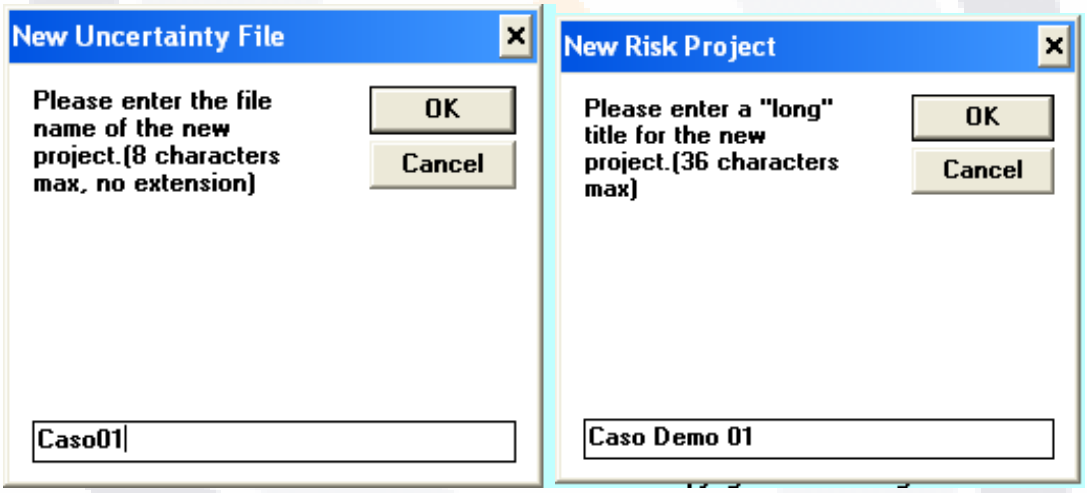
1.2 Crear archivo nuevo de tipo cualitativo.



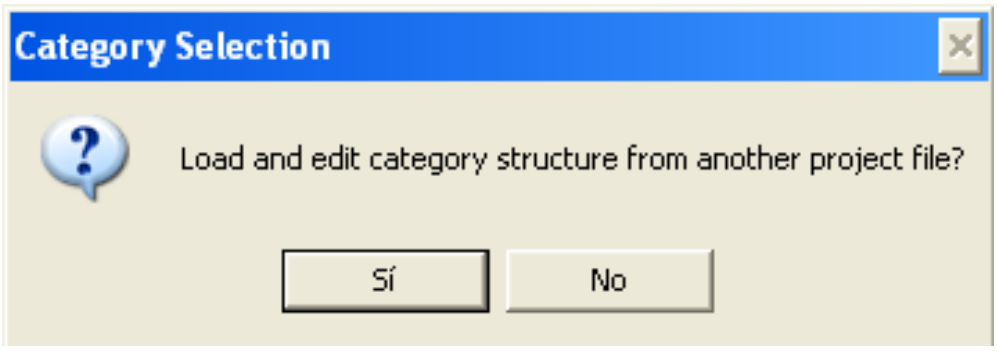
1.3 El sistema preguntará si se crea un archivo de opciones nuevo. Debemos indicar que si.



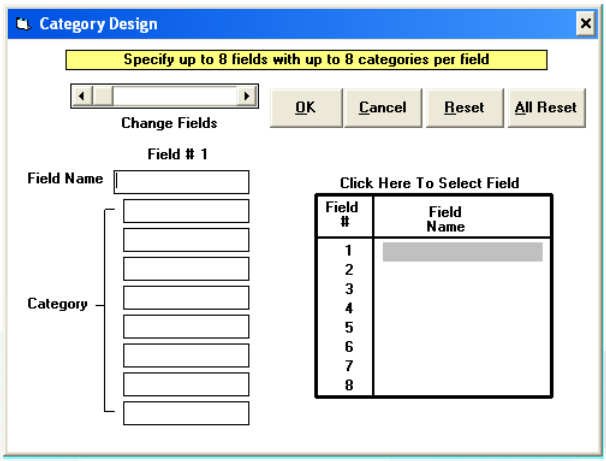
1.4 Se preguntaran 2 nombres: un nombre corto para el archivo de riesgos (New Uncertainty File) y un nombre largo. En este ejemplo se indica: Caso01 y Caso Demo 01, respectivamente.



1.5 El sistema demo preguntará si se usará la Clasificación de Categorías de Riesgos de otro Proyecto. Debemos indicar que no (en este ejemplo).



1.6 El sistema desplegará una forma con datos iniciales de una Clasificación de Riesgos. Debemos indicar <ALL RESET> para capturar datos nuevos.



1.6 Para este ejemplo podemos capturar los siguientes datos:

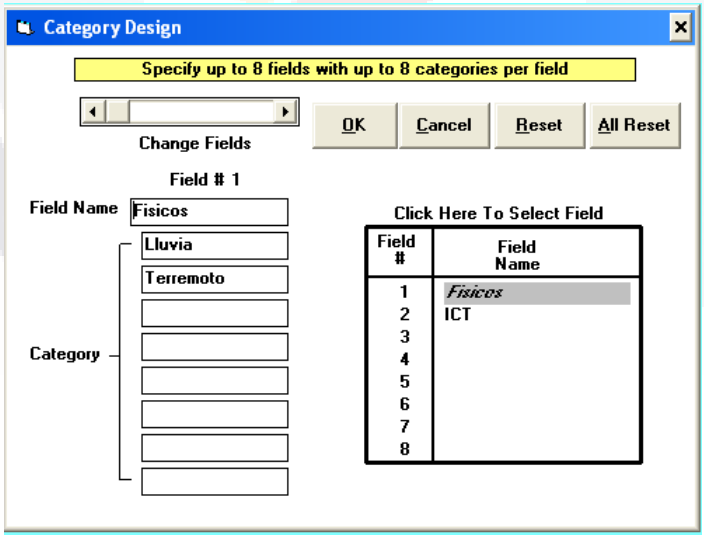
Físicos (field #1)

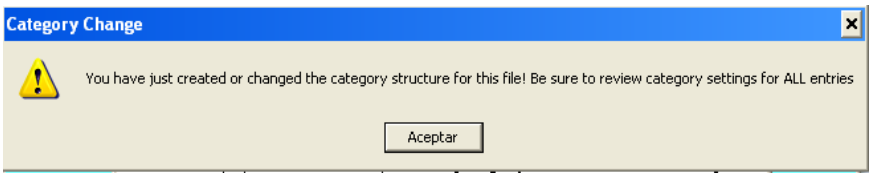
- Lluvia
- Terremotos

ICT (Hw, Sw,Red): (field #2)

- Uso inadecuado de Hw.
- Uso inadecuado de la de red de comunicación

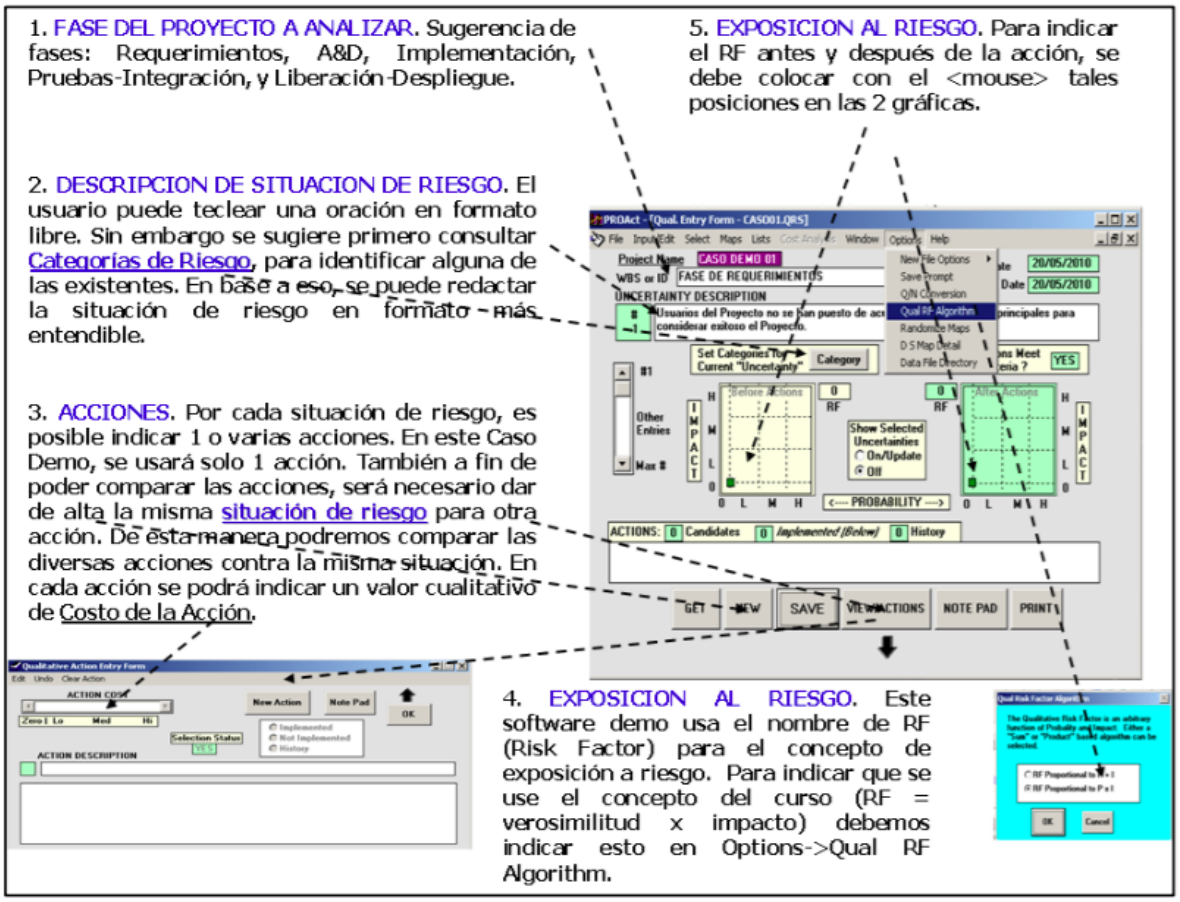
(para finalizar indicar <OK> y posterior mente <Aceptar>)





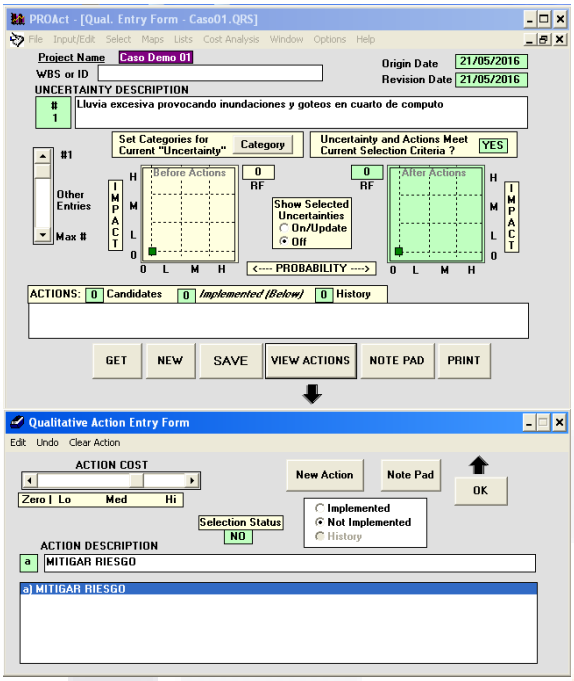
2. Captura de Situaciones (Riesgos) y Acciones contra Riesgos.

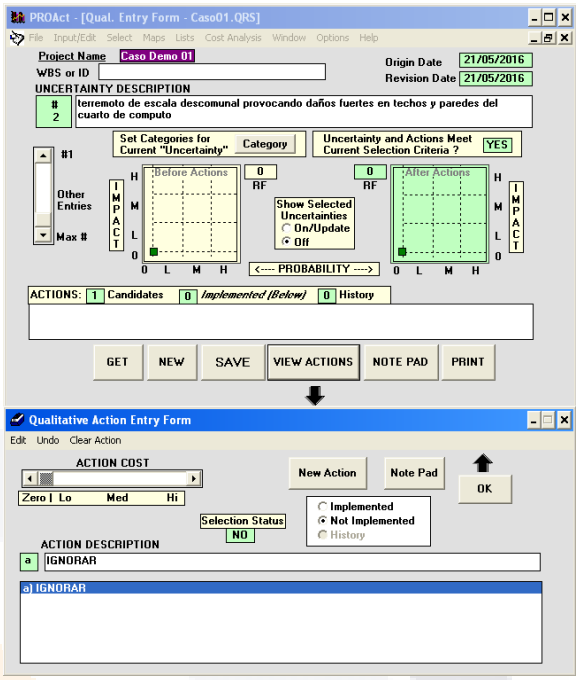
2.1 Ahora estamos listos para introducir los riesgos y las acciones contra riesgos a analizar. Sin embargo, es importante primero entender la forma de captura de datos como sigue:



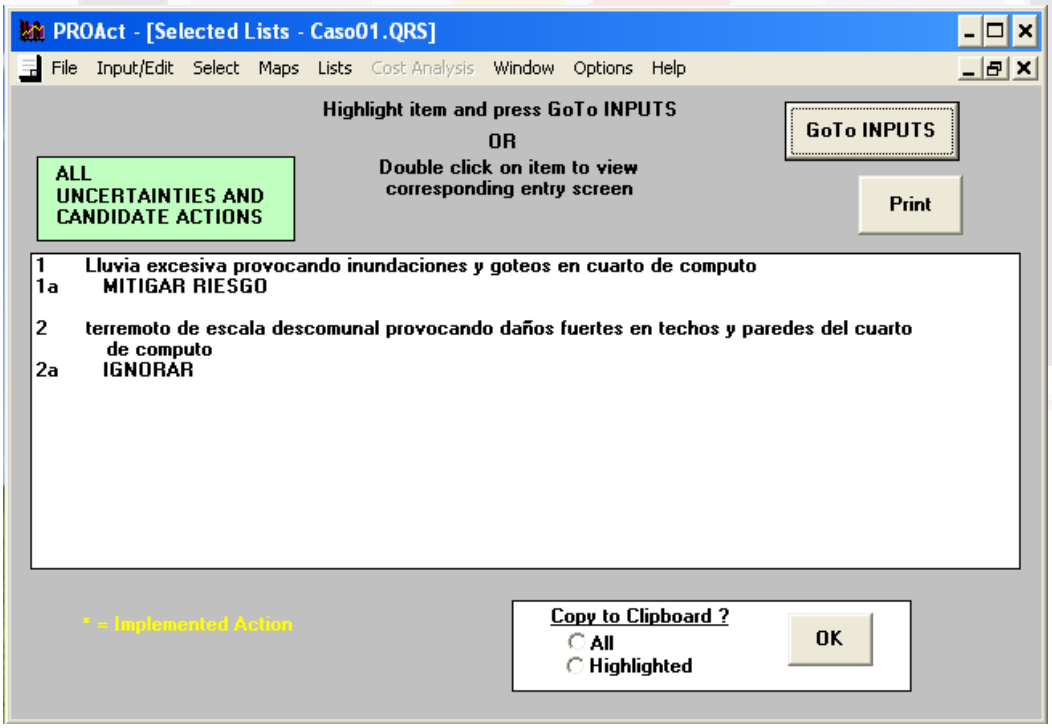
2.2 En base a lo anterior, en este caso Demo 01, analizaremos 2 situación de riesgo con 1 acción posible (el demo solo permite 10 datos). La situación de riesgo en este demo es el caso de un Data Center ubicado en la ciudad de Aguascalientes, Aguascalientes. En este ejemplo, en <Category> seleccionaremos solo <Lluvia>, y la situación: "Lluvia excesiva provocando inundaciones y goteos en cuarto de computo " de igual forma, en <Category> seleccionaremos solo <Terremoto>, y la situación: "Terremoto de escala descomunal provocando daños fuertes en techos y paredes del cuarto de computo"

2.3 Ahora daremos de alta las 2 acciones. Una acción para cada situación de riesgo Empezando para situación #1, en <VIEW ACTIONS>, para agregar la acción usamos <NEW ACTION>. El dato para #1 es A.1 MITIGAR RIESGO . Se debe también indicar el costo cualitativo de la acción (ACTION COST). Los valores posibles son: cero (Zero), bajo (Low), medio (Med) o alto (High). Es posible indicar valores intermedios: algo medio entre Lo-Med, y algo alto entre Med-Hi. Para la situación #2, en <VIEW ACTIONS>, para agregar la acción usamos <NEW ACTION>. El dato para #2 es A.2 IGNORAR RIESGO. Se debe también indicar el costo cualitativo de la acción (ACTION COST).





Al finalizar, con opción <Lists: Uncertainties with actions: All> obtendremos una lista de las 2 situaciones y las 2 acciones como sigue:

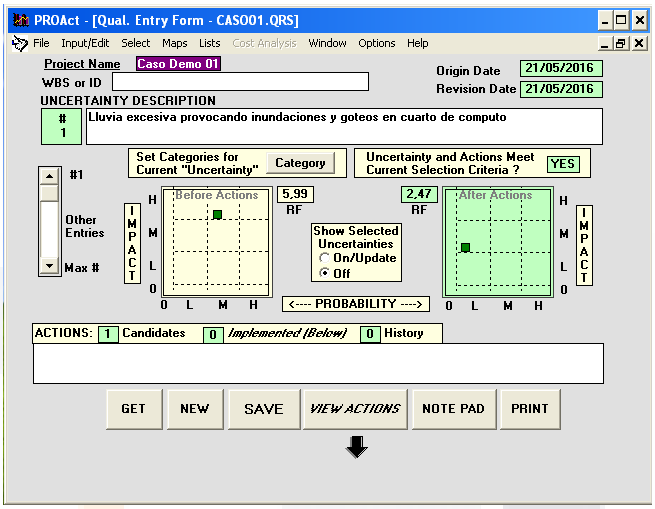


2.4 Ahora debemos estimar los niveles de exposición de riesgo (RF: risk factor) para cada caso antes y después de aplicar la estrategia.

A.1 MITIGAR RIESGO: MED-Hi

RF ANTES: 5.99

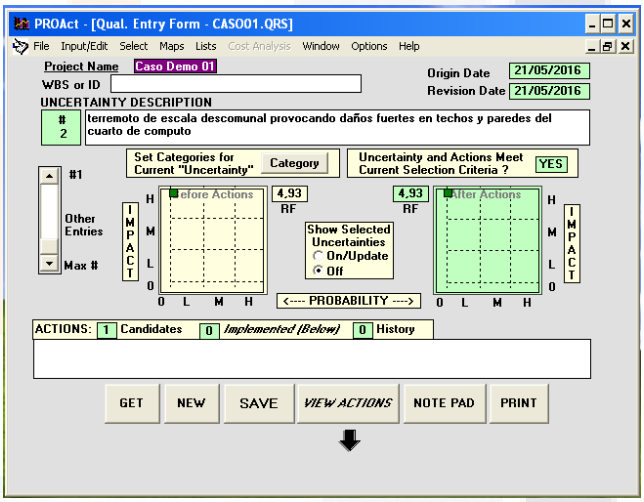
RF DESPUES: 2.47



A.2 IGNORAR: LOW

RF ANTES: 4.93

RF DESPUES: 4.93



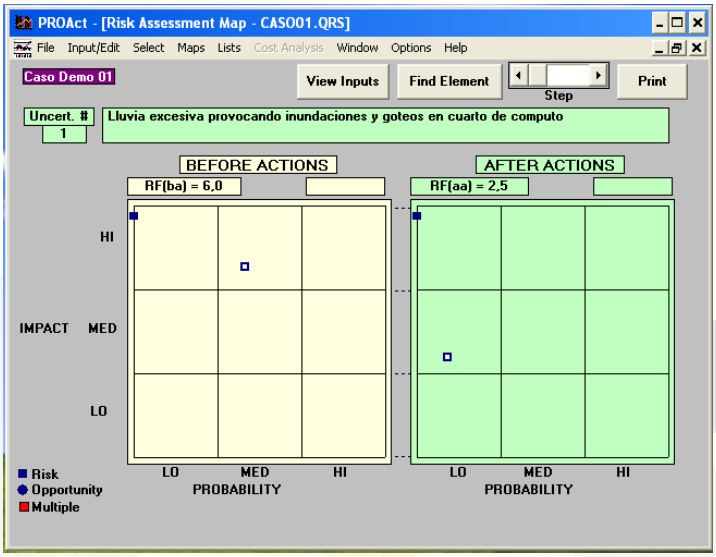
3. Análisis de Riesgos.

3.1 Ahora podemos ejecutar algunos análisis que permite el software demo.

3.2 Visualización de Mapa de Riesgos:

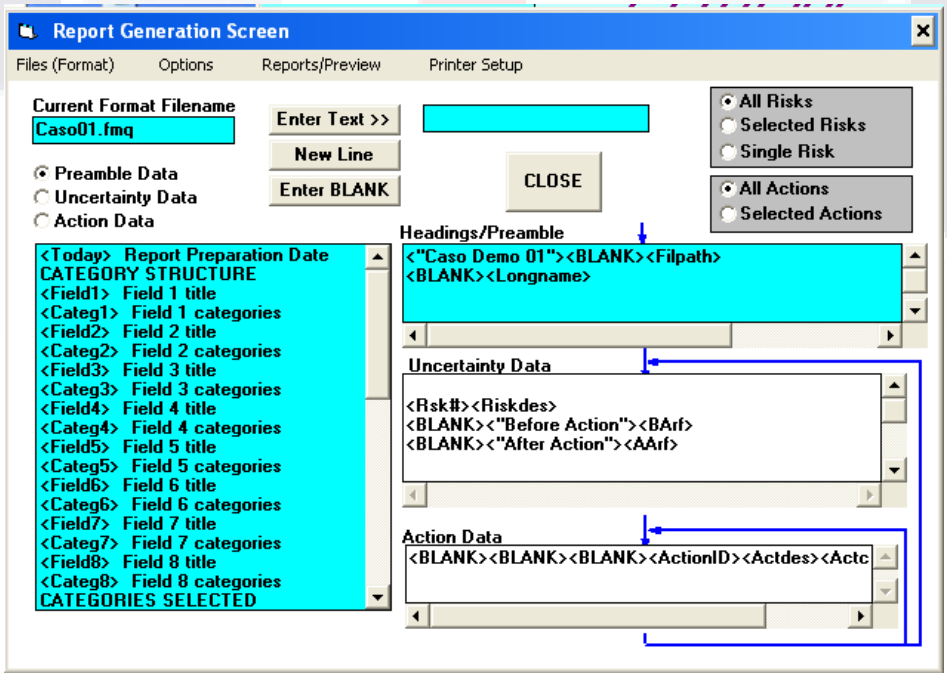
Esta opción se ejecuta con la opción <Maps : Risk Assessment>. La barra de <Step> permite avanzar de situación de riesgo a la siguiente. En nuestro demo, esto avanza a la otra situación 2. En la pantalla

podemos visualizar que los cuadros (antes y después) parpadean. Para visualizar esto se sugiere mejor imprimir el mapa, ya que cada situación (cuadro) es reportada con un numero progresivo.

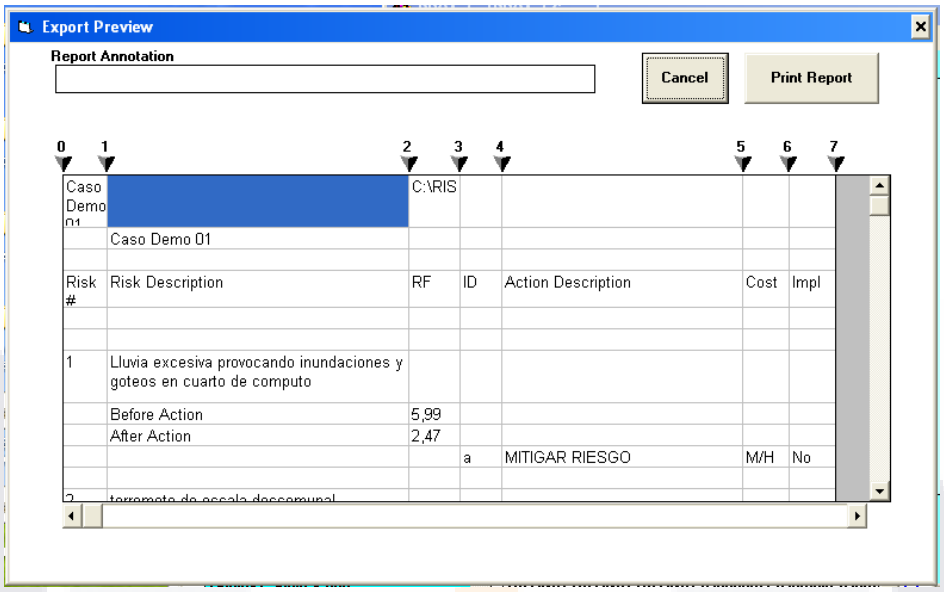


3.3 Impresión de Reporte (Formato Predefinido).

Esta opción se ejecuta con la opción <File : Report Generator>. Se abre el formato de ejemplo con <Files(Format) : Open : Qualitative> y seleccionar archivo tutor.fmq. Una vez abierto podemos cambiar el nombre a Caso01.fmq, y poner el título del reporte en <ENTER TEXT> como Caso Demo 01.

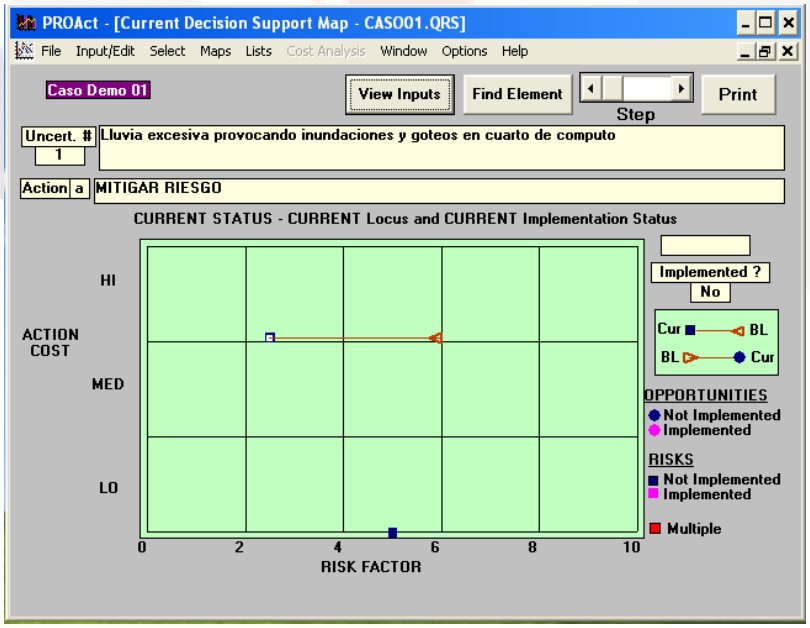


Para imprimirlo seleccionar <Reports/Previews : Print Report>. En este ejemplo esto produce el siguiente reporte:



3.3 Visualización de Mapa Comparativo.

Esta opción se ejecuta con la opción < Maps : Decision Support : Current >. Existe la opción de <Maps: Decision Support : Baseline> para mostrar solo la situación antes. La primer opción comentada muestra antes y después. Para avanzar sobre cada acción debe indicarse en <Step>.



Anexo B .- Formato de Reporte de control

Reporte de control

Inicio de Acciones de contramedida: _____
Fin de Acciones de contramedida: _____

Amenaza ID: _____
Acciones Dañinas: _____
Punto de inicio:
Daño: _____
Probabilidad: _____
Exposición al Riesgo: _____

Contramedida: _____
Después de aplicación de contramedida:
Daño: _____
Probabilidad: _____
Exposición al Riesgo: _____

Responsable de acción(es): _____
Status de la(s) acción(es): _____

Nombre del auditor: _____
Fecha de revisión: _____

Anexo C .- Tabla de la Distribución t

Distribution of *t* for Given Probability Levels

	Level of Significance for One-Tailed Test					
	.10	.05	.025	.01	.005	.0005
	Level of Significance for Two-Tailed Test					
d.f.	.20	.10	.05	.02	.01	.001
1	3.078	6.314	12.706	31.821	63.657	636.619
2	1.886	2.920	4.303	6.965	9.925	31.598
3	1.638	2.353	3.182	4.541	5.841	12.941
4	1.533	2.132	2.776	3.747	4.604	8.610
5	1.476	2.015	2.571	3.365	4.032	6.859
6	1.440	1.943	2.447	3.143	3.707	5.959
7	1.415	1.895	2.365	2.998	3.499	5.405
8	1.397	1.860	2.306	2.896	3.355	5.041
9	1.383	1.833	2.262	2.821	3.250	4.781
10	1.372	1.812	2.228	2.764	3.169	4.587
11	1.363	1.796	2.201	2.718	3.106	4.437
12	1.356	1.782	2.179	2.681	3.055	4.318
13	1.350	1.771	2.160	2.650	3.012	4.221
14	1.345	1.761	2.145	2.624	2.977	4.140
15	1.341	1.753	2.131	2.602	2.947	4.073
16	1.337	1.746	2.120	2.583	2.921	4.015
17	1.333	1.740	2.110	2.567	2.898	3.965
18	1.330	1.734	2.101	2.552	2.878	3.992
19	1.328	1.729	2.093	2.539	2.861	3.883
20	1.325	1.725	2.086	2.528	2.845	3.850
21	1.323	1.721	2.080	2.518	2.831	3.819
22	1.321	1.717	2.074	2.508	2.819	3.792
23	1.319	1.714	2.069	2.500	2.807	3.767
24	1.318	1.711	2.064	2.492	2.797	3.745
25	1.316	1.708	2.060	2.485	2.787	3.725
26	1.315	1.706	2.056	2.479	2.779	3.707
27	1.314	1.703	2.052	2.473	2.771	3.690
28	1.313	1.701	2.048	2.467	2.763	3.674
29	1.311	1.699	2.045	2.462	2.756	3.659
30	1.310	1.697	2.042	2.457	2.750	3.646
40	1.303	1.684	2.021	2.423	2.704	3.551
60	1.296	1.671	2.000	2.390	2.660	3.460
120	1.289	1.658	1.980	2.358	2.617	3.373
∞	1.282	1.645	1.960	2.326	2.576	3.291

Anexo D .- Servicios en http://148.211.145.149

UNIVERSIDAD AUTONOMA DE AGUASCALIENTES

CATALOGO DE SERVICIOS DE TI – 2015-1

LABORATORIO DATA CENTER
DEPTO. DE SISTEMAS DE INFORMACION
CENTRO DE CIENCIAS BASICAS

FORMA DE SOLICITUD DE SERVICIO DE TI

ITS ID	STATUS DEL SERVICIO	SERVICIO DE TI	MODO DE CONEXIÓN	DESCRIPCION	USUARIOS	BENEFICIOS	REQUERIMIENTOS GENERALES	SLA	RECURSOS DE APRENDIZ
1. SERVICIOS GENERALES DE TI									
1.1	ACTIVO	BIBLIOTECA DE HERRAMIENTAS DE TI	HTTP	COLECCIÓN DE HERRAMIENTAS DE TI DE ACCESO ACADÉMICO Y/O OPEN SOURCE	CARRERAS LTI/LITC. MAESTRÍA MITC. ACADEMIAS DSI. CUERPOS ACADÉMICOS DSI.	PROVEER UN DEPÓSITO COMÚN DE INVENTARIO DE HERRAMIENTAS DE TI DE LIBRE ACCESO ACADÉMICO	BROWSER FIREFOX + JRE 6	SLA-ITS.1.1	· NO REQUERIDO
1.2	ACTIVO	PORTAL GENERAL	HTTP	PORTAL LIFERAY GENERAL CON LINKS A PORTALES DE MTIC, CA-GESTI, DICC, LTI/LITC, Y SA-MITC.	CARRERAS LTI/LITC. MAESTRÍA MITC. ACADEMIAS DSI. CUERPOS ACADÉMICOS DSI.	PROVEER UN ESPACIO DE COMUNICACIÓN ENTRE DSI Y SUS USUARIOS	BROWSER FIREFOX + JRE 6	SLA-ITS.1.2	· GUIA
1.3	ACTIVO	MOODLE II	HTTP	LMS MOODLE PARA CURSOS CORTOS DE TI, CURSOS DE LTI/LITC Y CURSOS DE MITC	CARRERAS LTI/LITC. MAESTRÍA MITC.	PROVEER UN ESPACIO DE TIPO LMS	BROWSER FIREFOX + JRE 6	SLA-ITS.1.3	· GUIA
2. SERVICIOS DE SERVIDORES DE BASES DE DATOS									
2.1	ACTIVO	SERVIDOR.01 DE BASE DE DATOS MYSQL 5.5	TCP/IP	SERVIDOR DE BASE DE DATOS MYSQL 5.5 PARA USO REMOTO	CARRERAS LTI/LITC.	DISPONIBILIDAD DE SERVICIO DE BASES DE DATOS DE ACCESO REMOTO	MYSQL-GUI-TOOLS O MYSQL-WORKBENCH	SLA-ITS.2.1	· GUIA · TUTORIAL · CURSO · MYSQLTOOLS GUIA · MYSQL WORKBENCH G
2.2	ACTIVO	SERVIDOR.02 DE BASE DE DATOS MYSQL 5.5	TCP/IP	SERVIDOR DE BASE DE DATOS MYSQL 5.5 PARA USO REMOTO	CARRERAS LTI/LITC.	DISPONIBILIDAD DE SERVICIO DE BASES DE DATOS DE ACCESO REMOTO	MYSQL-GUI-TOOLS O MYSQL-WORKBENCH	SLA-ITS.2.2	· GUIA · TUTORIAL · CURSO · MYSQLTOOLS GUIA · MYSQL WORKBENCH G
2.3	ACTIVO	SERVIDOR.03 DE BASE DE DATOS MYSQL 5.5	TCP/IP	SERVIDOR DE BASE DE DATOS MYSQL 5.5 PARA USO REMOTO	MAESTRÍA MITC.	DISPONIBILIDAD DE SERVICIO DE BASES DE DATOS DE ACCESO REMOTO	MYSQL-GUI-TOOLS O MYSQL-WORKBENCH	SLA-ITS.2.3	· GUIA · TUTORIAL · CURSO · MYSQLTOOLS GUIA · MYSQL WORKBENCH G
2.4	ACTIVO	SERVIDOR.01 DE BASE DE DATOS MS-SQL EXPRESS ADVANCED 2008R2	TCP/IP	SERVIDOR DE BASE DE DATOS MS-SQL EXPRESS 2008 PARA USO REMOTO	CARRERAS LTI/LITC.	DISPONIBILIDAD DE SERVICIO DE BASES DE DATOS DE ACCESO REMOTO	SQL MANAGEMENT STUDIO TOOL	SLA-ITS.2.4	· MS GUIDE · SQL MANAGEMENT STUDIO TUTORIAL
2.5	ACTIVO	SERVIDOR.02 DE BASE DE DATOS MS-SQL 2008R2 STANDARD + BI TOOLS	TCP/IP	SERVIDOR DE BASE DE DATOS MS-SQL 2008R2 STANDARD + BI TOOLS PARA USO REMOTO	MAESTRÍA MITC.	DISPONIBILIDAD DE SERVICIO DE BASES DE DATOS DE ACCESO REMOTO	SQL MANAGEMENT STUDIO TOOL	SLA-ITS.2.5	· MS GUIDE · SQL MANAGEMENT STUDIO TUTORIAL · BI DEVELOPMENT STUD GUIA · BI PRESENTACION · FREEE BOOK BI
· 3. SERVICIOS DE SERVIDORES DE APLICACIONES JAVA									
3.1	ACTIVO	SERVIDOR.01 DE APPS TOMCAT 7.0	HTTP	SERVIDOR DE APLICACIONES JAVA TOMCAT 7.0 PARA USO REMOTO	CARRERAS LTI/LITC.	DISPONIBILIDAD DE SERVICIO DE SERVER DE APLICACIONES JAVA DE ACCESO REMOTO	BROWSER FIREFOX + JRE 6	SLA-ITS.3.1	· GUIA · EJEMPLOS · CURSO TOMCAT 7
3.2	ACTIVO	SERVIDOR.02 DE APPS TOMCAT 7.0	HTTP	SERVIDOR DE APLICACIONES JAVA TOMCAT 7.0 PARA USO REMOTO	MAESTRÍA MITC.	DISPONIBILIDAD DE SERVICIO DE SERVER DE APLICACIONES JAVA DE ACCESO REMOTO	BROWSER FIREFOX + JRE 6	SLA-ITS.3.2	· GUIA · EJEMPLOS · CURSO TOMCAT 7
3.3	ACTIVO	SERVIDOR.01 DE APPS GLASSFISH 3.1	HTTP	SERVIDOR DE APLICACIONES JAVA GLASSFISH 3.1 PARA USO REMOTO	CARRERAS LTI/LITC.	DISPONIBILIDAD DE SERVICIO DE SERVER DE APLICACIONES JAVA DE ACCESO REMOTO	BROWSER FIREFOX + JRE 6	SLA-ITS.3.3	· GUIA · EJEMPLOS · CURSO GLASSFISH
3.4	ACTIVO	SERVIDOR.02 DE APPS GLASSFISH 3.1	HTTP	SERVIDOR DE APLICACIONES JAVA GLASSFISH 3.1 PARA USO REMOTO	MAESTRÍA MITC.	DISPONIBILIDAD DE SERVICIO DE SERVER DE APLICACIONES JAVA DE ACCESO REMOTO	BROWSER FIREFOX + JRE 6	SLA-ITS.3.4	· GUIA · EJEMPLOS · CURSO GLASSFISH

4. SERVICIOS DE SERVIDORES DE REPORTES JAVA									
4.1	ACTIVO	SERVIDOR.01 DE REPORTES JASPER 4.7	HTTP	SERVIDOR DE REPORTES JASPER 4.7 PARA JAVA PARA USO REMOTO	CARRERAS LTI/LITC.	DISPONIBILIDAD DE SERVICIO DE SERVER JASPER 4.7 DE REPORTES JAVA DE ACCESO REMOTO	BROWSER FIREFOX + JRE 6 + JASPERSTUDIO + IREPORT	SLA-ITS.4.1	· GUIA · CURSO I · CURSO II · CURSO III
4.2	ACTIVO	SERVIDOR.02 DE REPORTES JASPER 4.7	HTTP	SERVIDOR DE REPORTES JASPER 4.7 PARA JAVA PARA USO REMOTO	MAESTRÍA MITC.	DISPONIBILIDAD DE SERVICIO DE SERVER JASPER 4.7 DE REPORTES JAVA DE ACCESO REMOTO	BROWSER FIREFOX + JRE 6 + JASPERSTUDIO + IREPORT	SLA-ITS.4.2	· GUIA · CURSO I · CURSO II · CURSO III
5. SERVICIOS DE SERVIDORES DE WEB IIS 7.0									
5.1	ACTIVO	SERVIDOR.01 WEB IIS 7.0	HTTP	SERVIDOR WEB IIS 7.0 (PHP HABILITADO)	CARRERAS LTI/LITC.	DISPONIBILIDAD DE SERVICIO SERVER WEB IIS 7.0 HABILITADO CON PHP	BROWSER IEXPLORER + JRE 6	SLA-ITS.5.1	· TUTORIAL · GUIA
5.2	ACTIVO	SERVIDOR.02 WEB IIS 7.0	HTTP	SERVIDOR WEB IIS 7.0 (PHP HABILITADO)	MAESTRÍA MITC.	DISPONIBILIDAD DE SERVICIO SERVER WEB IIS 7.0 HABILITADO CON PHP	BROWSER IEXPLORER + JRE 6	SLA-ITS.5.2	· TUTORIAL · GUIA
6. SERVICIOS DE SERVIDORES DE VISUAL STUDIO 2010									
6.1	ACTIVO	VISUAL STUDIO 2010	RDP	VISUAL STUDIO 2010 PROFESIONAL (C#, VB, VWEB)	CARRERAS LTI/LITC.	DISPONIBILIDAD DE ACCESO REMOTO A PLATAFORMA DE VISUAL STUDIO 2010 PROFESIONAL	WINDOWS REMOTE DESKTOP CONNECTION TOOL	SLA-ITS.6.1	· GUIA · CURSO C# · CURSO MS-SQL REP
6.2	ACTIVO	VISUAL STUDIO 2010	RDP	VISUAL STUDIO 2010 PROFESIONAL (C#, VB, VWEB)	MAESTRÍA MITC.	DISPONIBILIDAD DE ACCESO REMOTO A PLATAFORMA DE VISUAL STUDIO 2010 PROFESIONAL	WINDOWS REMOTE DESKTOP CONNECTION TOOL	SLA-ITS.6.2	· GUIA · CURSO C# · CURSO MS-SQL REP
7. SERVICIOS DE APLICACIONES OPEN SOURCE									
7.1	ACTIVO	APLICACIÓN DE ERP.01	HTTP	ERP OPEN SOURCE BÁSICO PARA PYMES DE MANUFACTURA Y SERVICIOS	CARRERAS LTI/LITC.	DISPONIBILIDAD DE ACCESO REMOTO A PLATAFORMA WEB ERP CON MÓDULOS BÁSICOS PARA PYMES	BROWSER FIREFOX + JRE 6	SLA-ITS.7.1	· GUIA · CURSO
7.2	ACTIVO	APLICACIÓN DE ERP.02	HTTP	ERP OPEN SOURCE BÁSICO PARA PYMES DE MANUFACTURA Y SERVICIOS	MAESTRÍA MITC.	DISPONIBILIDAD DE ACCESO REMOTO A PLATAFORMA WEB ERP CON MÓDULOS BÁSICOS PARA PYMES	BROWSER FIREFOX + JRE 6	SLA-ITS.7.2	· GUIA · CURSO
7.3	ACTIVO	APLICACIÓN DE CRM – EPESI.01	HTTP	CRM-EPESI OPEN SOURCE BÁSICO PARA PYMES	CARRERAS LTI/LITC.	DISPONIBILIDAD DE ACCESO REMOTO A PLATAFORMA CRM PARA PYMES	BROWSER FIREFOX + JRE 6	SLA-ITS.7.3	· GUIA · MANUAL
7.4	ACTIVO	APLICACIÓN DE CRM – EPESI.02	HTTP	CRM-EPESI OPEN SOURCE BÁSICO PARA PYMES	MAESTRÍA MITC.	DISPONIBILIDAD DE ACCESO REMOTO A PLATAFORMA CRM PARA PYMES	BROWSER FIREFOX + JRE 6	SLA-ITS.7.4	· GUIA · MANUAL
7.5	ACTIVO	APLICACIÓN DE GESTIÓN DE PROYECTOS.01	HTTP	APLICACIÓN WEB OPEN SOURCE WEB2PROJECT DE GESTIÓN DE PROYECTOS	CARRERAS LTI/LITC.	DISPONIBILIDAD DE ACCESO REMOTO A PLATAFORMA WEB PARA GESTIÓN DE PROYECTOS	BROWSER FIREFOX + JRE 6	SLA-ITS.7.5	· GUIA
7.6	ACTIVO	APLICACIÓN DE GESTIÓN DE PROYECTOS.02	HTTP	APLICACIÓN WEB OPEN SOURCE WEB2PROJECT DE GESTIÓN DE PROYECTOS	MAESTRÍA MITC.	DISPONIBILIDAD DE ACCESO REMOTO A PLATAFORMA WEB PARA GESTIÓN DE PROYECTOS	BROWSER FIREFOX + JRE 6	SLA-ITS.7.6	· GUIA

Anexo E .- Video Complemento de la Implementación del Caso LabDC-UAA: Servicio Moodle II

Como complemento de la tesis para la evaluación del proceso, se utilizó el caso demo del LabDC-UAA apoyado por un video para demostrar la implementación y uso de la herramienta de apoyo PROAct, con el objetivo de proveer una mejor apreciación de la utilidad de los mismos (proceso y herramienta de apoyo). Esto se anexa en el DISCO COMPLEMENTO de esta Tesis.