SOFTWARE DE APOYO AL PROCESO DE CREACIÓN Y REGISTRO DE POLÍTICAS DE SEGURIDAD INFORMÁTICA EN ORGANIZACIONES

Investigadores
YESSICA JULIE MARRUGO MARRUGO (UNICARTAGENA)
RONALD NUÑEZ BARCOS (UNICARTAGENA)

UNIVERSIDAD DE CARTAGENA
FACULTAD DE INGENIERÍA
INGENIERÍA DE SISTEMAS
CARTAGENA DE INDIAS, 2012

SOFTWARE DE APOYO AL PROCESO DE CREACIÓN Y REGISTRO DE POLÍTICAS DE SEGURIDAD INFORMÁTICA EN ORGANIZACIONES

PROYECTO DE GRADO

GRUPO DE INVESTIGACIÓN GIMÁTICA
Tecnologías de las Comunicaciones e Informática

Investigadores
YESSICA JULIE MARRUGO MARRUGO (UNICARTAGENA)
RONALD NUÑEZ BARCOS (UNICARTAGENA)

Tutor
RAÚL JOSÉ MARTELO GÓMEZ (UNICARTAGENA)

UNIVERSIDAD DE CARTAGENA
FACULTAD DE INGENIERÍA
INGENIERÍA DE SISTEMAS
CARTAGENA DE INDIAS, 2012

UNIVERSIDAD DE CARTAGENA

Proyecto de Grado: SOFTWARE DE APOYO AL PROCESO DE CREACIÓN Y REGISTRO DE POLÍTICAS DE SEGURIDAD INFORMÁTICA EN ORGANIZACIONES

Autores: YESSICA JULIE MARRUGO MARRUGO
RONALD NUÑEZ BARCOS

Tutor: RAÚL JOSÉ MARTELO GÓMEZ

Nota de Aceptación

_____

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

Cartagena de Indias, ____ de _____ de 2012

RESUMEN

Los resultados de las últimas encuestas realizadas por la Asociación Colombiana de Ingenieros de Sistemas, ACIS , particularmente la X Encuesta Nacional sobre Seguridad Informática en Colombia (2010) indica que existen múltiples fallas de seguridad en organizaciones nacionales, debido principalmente a virus, uso de software no autorizado, accesos no autorizados a la Web, y la fuga de información. Adicionalmente, el 66,19% de las empresas no tienen políticas de seguridad informática formalmente definidas, es decir, escritas, documentadas e informadas al personal. A la luz de la evidencia presentada, es claro que las organizaciones experimentan pérdida de datos y fallas en sus sistemas, que pueden ser inducidos por la falta de implantación de esquemas de seguridad flexibles fundamentados en Políticas de Seguridad Informática (PSI) bien estructuradas.

Ante esta situación, las políticas de seguridad requieren alto grado de atención y esfuerzo conjunto entre la administración y el área de sistemas de las organizaciones. Se requieren mecanismos que apoyen la tarea de creación de PSI, con el propósito de hacerla menos tediosa y atenuar la complejidad asociada a la selección y aplicación de metodologías o estándares relacionados, de tal forma que se contemple la seguridad en la información, redes y sistemas computacionales.

Para lograrlo, el presente proyecto tiene como objetivo Desarrollar un Software de Apoyo en el Proceso de Creación, Redacción, Clasificación y Registro de Políticas de Seguridad Informática en Organizaciones, basado en el estudio de diferentes normas y estándares existentes para el establecimiento de PSI. El fundamento teórico se centra en definir aspectos relacionados con objetivos, elementos y compromisos de la Seguridad Informática, conceptos y ciclo de vida de las políticas, así como estándares internacionales más destacados en la actualidad.

Con la ejecución del mismo se obtuvo un informe detallado de los resultados, donde se especificó estrategias destacadas en cada uno de los modelos, estándares y/o normas estudiadas, los cuadros de análisis construidos, y la descripción de características del

esquema propuesto. Además, el software que servirá de guía en las organizaciones, anexando los datos relevantes de la prueba aplicada.

Palabras Clave:

Políticas de Seguridad Informática, Esquema, Seguridad Física, Estándares

ABSTRACT

The results of recent surveys conducted by the Colombian Association of Engineers Systems, ACIS, particularly the Tenth National Computer Security Survey in Colombia (2010) indicates that there are multiple security flaws in national organizations, mainly due to viruses, use of software unauthorized, unauthorized access to the Web, and information leakage. Additionally, 66.19% of companies have no formal information security policies defined, ie, written, documented and reported to staff. In light of the evidence presented, it is clear that organizations experience data loss and failures in their systems, which can be induced by the lack of implementation of flexible security schemes grounded in Computer Security Policy (ISP) or structured.

In this situation, the security policies require a high degree of attention and effort between the administration and the area of systems of organizations. Mechanisms are needed to support the task of creating PSI, in order to make it less tedious and reduce the complexity associated with the selection and application of methodologies and standards related, so that consideration of information security, networks and systems computer.

To achieve this, this project aims to develop a Software Support in the Process of Creation, Structure, Classification and Registration of Information Security Policies in Organizations, based on the study of several existing norms and standards for the establishment of PSI. The foundation focuses on theoretical aspects define objectives, elements and commitments of Computer Security, concepts and life cycle policies and international standards currently outstanding.

With the execution of it was obtained a detailed report of the results, which highlighted strategies specified in each of the models, standards and / or standards studied, analysis tables built, and the description of features of the proposed scheme. In addition, the software will guide organizations, attaching the relevant data from the test applied.

Key Words:

Information Security Policies, Schematic, Physical Security, Standards

DEDICATORIA

A Dios nuestro señor y la Virgen María, por cada día iluminar nuestro camino y brindarnos la oportunidad de seguir, de luchar, y fortalecernos para culminar esta meta.

A nuestros padres y familiares, por su entrega en este trabajo como si fuese propio, con gran esfuerzo, amor y sacrificios constantes que nunca olvidaremos, mostrándonos con una sonrisa que el verdadero amor existe.

A nuestros amigos, por acompañarnos en esta labor de forma incondicional, compartiendo momentos difíciles, y de alegrías que llenaban nuestros corazones de fuerza, sin duda son una luz brillando en la oscuridad.

A nuestros docentes, que con paciencia y dedicación nos enseñaron las mejores lecciones de la vida, aquellas que nos hacen mejores personas, aprendimos que no hay camino difícil, cuando perseveramos y somos pacientes vemos los frutos del esfuerzo.

A nuestro tutor, Raúl, alguien que con profesionalismo, entusiasmo, buen sentido del humor y sabios consejos nos guió en el camino, además de profesor es nuestro amigo y compañero de lucha.

AGRADECIMIENTOS

Nuestra gratitud está dirigida principalmente a Dios por habernos brindado lo necesario en el momento justo, para lograr este paso. A nuestros padres por su apoyo incondicional y lucha incansable por vernos crecer a diario.

Deseamos agradecer a nuestro tutor, Raúl José Martelo Gómez su apoyo, paciencia, confianza, orientación y trabajo, gracias a sus ideas e impecable dirección esta investigación ha logrado resultados satisfactorios.

Agradecemos a la Universidad de Cartagena, cómo el alma máter que nos acogió, mediante cada una de las personas que hacen parte de ella, y de cualquier modo aportaron un granito de arena a nuestro trabajo, durante estos años.

Agradecimientos sinceros al Doctor Álvaro Gómez Vieites, por sus oportunos aportes e incondicional acompañamiento.

Gracias, al grupo de investigación Gimática, Semillero GinRed, su apoyo, y aporte valioso; a los docentes Yasmín Moya Villa, Plinio Puello Marrugo, Humberto Caicedo Blanco y Luis C. Tovar Garrido por ayudarnos a enriquecer el proyecto.

Sin olvidar, a nuestros grandes amigos y aliados María Macareno, Edelberto Reyes, Julissa Mendoza, Mayker Pájaro, Jesús D. Rodríguez, Camilo Velásquez, Iván D. Romero, José Llamas, Alonso Montenegro, Beatriz Benítez, Verónica González, Francisco Carreño, Luis G. Díaz Villalobos, Ana Tarrá, Gennys Carrasquilla, Hamid Pinilla, Pedro Ruiz, Carlos Cuadrado, Jorge Buendía, Marco González, Rafael Sánchez y todos aquellos que no aparecen en lista pero igualmente ocupan un lugar especial en nuestros corazones.

CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

El presente proyecto está dirigido al estudio de diferentes modelos, normas y estándares destacados en la actualidad para la definición de Políticas de Seguridad Informática en organizaciones, forjando su impacto a la ciudad de Cartagena / Colombia, inicialmente.

El interés de la investigación en el área se debe, principalmente, al auge de problemas de inseguridad en la información, suscitados a partir de los avances que han tenido las redes y sistemas computacionales. Además, al desinterés mostrado por las empresas en cuanto al tema de políticas de seguridad, o inversiones en la seguridad de sus sistemas de cómputo, donde se almacena gran parte de la información crítica que permite la estabilidad y continuidad del negocio. Esto se evidencia en los diferentes estudios estadísticos realizados cada año por la Asociación Colombiana de Ingenieros de Sistemas (ACIS), tratados más adelante en el Marco teórico. Igualmente, se refleja en la falta de proyectos, a nivel local y/o nacional, orientados al establecimiento de modelos de seguridad de la información. De hecho, actualmente en la ciudad de Cartagena no aparecen registros en la web que indiquen estudios relacionados; generalmente, se hace referencia a las normas internas de la empresa.

Las políticas de seguridad informática (PSI) como parte fundamental de los Sistemas de Gestión de Seguridad de la Información (SGSI) constituyen un canal formal de actuación, en relación a los recursos y servicios informáticos de la organización, que permiten establecer reglas que regulan la forma en que la organización previene los riesgos. Sin embargo, el proceso de creación se torna complejo cuando se está en frente de múltiples normas, modelos, estándares que hablan de todo tipo de formas, pero no se sabe cuál es la más adecuada, ni los pasos para empezar. De allí surge, el interrogante: ¿Cómo reducir la complejidad asociada a la aplicación de modelos ya existentes para la creación, redacción, clasificación, y registro de políticas de seguridad informática en las organizaciones?

En respuesta a ello, la investigación propuesta tiene como objetivo *Desarrollar un Software de Apoyo en el proceso de Creación, Redacción, Clasificación y Registro de Políticas de*

Seguridad Informática en las Organizaciones, que facilite, precisamente, esta difícil tarea. Para lograrlo, se aplica la siguiente estrategia metodológica:

Diseño y aplicación de instrumentos de recolección de información. Búsqueda y apropiación del conocimiento en estándares, normas, o modelos de gestión de Buenas Prácticas en Seguridad de la Información, destacando las normas internacionales ISO17799, e ISO 27001. Posterior construcción de cuadros comparativos y evaluaciones detalladas, que den lugar a la Estructuración de un Esquema básico de seguridad, que finalmente, es materializado a través del Software que establece una serie de pasos por las diferentes etapas de creación de políticas de seguridad física.

Una vez obtenido el producto software, se realizan pruebas prácticas en la empresa de prestación de servicios AKENDOS S.A.S, y se documentan los resultados.

La implementación del modelo básico de seguridad informática mencionado, incluye una serie de pautas y recomendaciones a seguir para la definición de PSI a nivel de Seguridad Física en organizaciones, y un conjunto de etapas asociadas, mostradas de forma didáctica en la aplicación a desarrollar; representa no sólo una solución al problema de inseguridad informática enfrentado por las empresas actualmente, debido a la ausencia de principios o intenciones de alto nivel (*políticas de seguridad informática*) sino, que integra una serie de actividades de carácter documental, descriptivo, analítico y experimental que permitirá a los investigadores la adquisición de amplios conocimientos en el área de seguridad de la información, principalmente, en estándares, modelos o normas internacionales reconocidos mundialmente. Así mismo, representa la llave que abre muchas puertas al mercado laboral e investigativo, a nivel nacional e internacional, en la medida en que el proyecto sea divulgado y presentado en las empresas como opción atractiva y de fácil acceso, teniendo como precedente su carácter innovador.

1. OBJETIVOS Y ALCANCE

1.1. OBJETIVO GENERAL

Desarrollar un Software de Apoyo en el proceso de Creación, Redacción, Clasificación y Registro de Políticas de Seguridad Informática en las Organizaciones, basado en el estudio de los diferentes modelos, normas y estándares existentes para el establecimiento de políticas de seguridad.

1.2. OBJETIVOS ESPECÍFICOS

- Construir el estado del arte del proyecto, con base en información relacionada con políticas de seguridad informática, los diferentes estándares, normas o modelos que ofrecen recomendaciones para realizar la gestión de la seguridad de la información, con el fin de obtener un referente teórico y además requerimientos de la herramienta a desarrollar.
- Identificar las ventajas y desventajas de cada modelo, estándar y/o norma, y resaltar posibles estrategias a aplicar.
- Construir un Esquema básico de seguridad, con base en los aspectos relevantes encontrados en las investigaciones.
- Desarrollar un software que materialice el esquema construido a partir de las estrategias identificadas.
- Realizar un consolidado final de la investigación, donde se plasmen los resultados teóricos y prácticos.
- Divulgar aspectos representativos de la investigación.
- Presentar resultados experimentales del proyecto, a través de aplicación del esquema a una organización.

2. ESTADO Y TENDENCIAS DE LA SEGURIDAD INFORMÁTICA

La seguridad informática tiene lugar desde los primeros avances de las redes y sistemas computacionales, cuando se detectaron alteraciones desconocidas e inexploradas hasta entonces. Al realizar un breve recorrido por la historia, se rescatan sucesos relacionados con el origen de los virus, ataques, códigos maliciosos, hackers y su impacto en este ámbito:

Hacia 1986, dos personajes conocidos como Basit y Amjad descubrieron un código ejecutable en el boot de un disquete, que corría siempre que se reiniciaba el computador con el disco flexible en A; encontrando que éste podía instalarse fácilmente en memoria residente reemplazando un programa allí almacenado, además de ubicar una copia de sí mismo en cada disquete. Al ser alteraciones desconocidas, ellos las denominaron “virus” por la similitud con los virus biológicos (Virusprot, 2010).

A partir de este año, se conocieron diversos casos de mayor relevancia, que promovieron estudios en el campo. En 1987 la Universidad de Delaware determinó que tenía un virus cuando empezaron a ver una extraña y sospechosa 'etiqueta' que aparecía en los disquetes. Y eso es todo lo que este pequeño virus hacía (auto replicarse y colocar una 'etiqueta'). Ese mismo año, Franz Swoboda tuvo noticia de un virus incluido en un programa llamado 'Charlie'. Mientras que en EEUU, Fred Cohen finalizaba su tesis doctoral relacionada con los virus informáticos conocidos, promoviendo la aparición de grupos de noticias sobre virus. *Por ello, le llamó el 'Virus Charlie'. Hubo mucho revuelo en la opinión pública acerca de este virus, al difundirse las dos versiones de una misma historia: Burger afirmó que había obtenido una copia del virus de manos de Swoboda, pero Swoboda lo negó siempre. El efecto fue que los archivos 'parcheados' colgaban el PC, en vez de reiniciarlo. No era una mejora muy satisfactoria* (Virusprot, 2010).

De esta forma, empezó el auge de virus informáticos y todo tipo de ataques a los sistemas, agravando cada vez la situación. Muestra de ello es que el 2 de noviembre de 1988, es

recordado como "el día en que el internet se detuvo**"** debido a que en esa fecha, un virus atacó Internet, ocasionando el primer ataque de denegación de servicio (DoS). Aunque sólo se vio comprometida el 10% de la red *Arpanet*, este gusano conocido como *Morris*, en alusión a su creador, descifraba contraseñas débiles, además de vulnerabilidades en la aplicación de correo electrónico Sendmail, en las utilidades de Unix finger y rsh, infectaba servidores consumiendo más recursos de CPU, degradando su servicio (Sandoval, 2010). Sin embargo, el hecho no sólo acarreó consecuencias negativas, sino que logró concienciar sobre el primitivo concepto de **Seguridad Informática**, lo que se reflejó en la creación de un equipo de respuesta a emergencias en sistemas computacionales llamado CERT (Computer Emergency Response Team).

Continuando la creciente secuencia de ataques, según las estadísticas, en 1997, el 54% de las empresas norteamericanas sufrieron ataques de Hackers[1] en sus sistemas, ocasionando pérdidas por 137 millones de dólares. Organismos mundiales como el Pentágono, la CIA, UNICEF, La ONU, entre otros, han sido víctimas de intrusiones por parte de los populares y temidos piratas informáticos (CEAS EDUCACION, 2010).

De esta forma, el desarrollo de la "sociedad de la información", de las tecnologías computacionales, y la adopción de internet como elemento de comunicación trajo consigo innumerables problemas de seguridad que debían ser atendidos para resguardar la confidencialidad, disponibilidad e integridad de la información, como uno de los activos principales en las organizaciones.

Ante esta situación, la seguridad informática nace como un área de la Computación que da respuesta a los inconvenientes y *"se enfoca en la protección de la infraestructura computacional y todo lo relacionado con ésta (incluyendo la información)"* (Wikipedia, 2010). En consecuencia, para garantizar que los recursos informáticos estén disponibles en el cumplimiento de sus propósitos, se debe contemplar la definición de un marco o esquema de seguridad eficiente bajo el concepto de seguridad informática, que implica el

[1] Del inglés hack. Término utilizado para llamar a una persona con grandes conocimientos en informática y telecomunicaciones y que los utiliza con un determinado objetivo.

cumplimiento y aplicación de una serie de estándares, protocolos, métodos, reglas, herramientas y leyes. Es decir, las organizaciones deben estar a la vanguardia de los procesos de cambio continuo de la sociedad, principalmente aquellas con alta dependencia en infraestructura tecnológica.

Uno de los componentes definidos, dentro de seguridad informática, con la finalidad de afrontar los ataques mencionados, reducir los niveles de vulnerabilidad, administrar eficientemente el riesgo y cumplir los propósitos descritos a nivel organizacional, ha sido el establecimiento de Políticas de Seguridad, conceptualizadas como "*La declaración de intenciones de alto nivel que cubre la seguridad de los sistemas informáticos y que proporciona las bases para definir y delimitar responsabilidades para las diversas actuaciones técnicas y organizativas que se requieran*" (Vieites, DIRECTRICES PARA LA DEFINICION E IMPLANTACION DE POLITICAS DE SEGURIDAD, 2009).

A través de los años, el interés por la determinación e implantación de políticas ha sido creciente; sin embargo, los estudios demuestran que los problemas también se han multiplicado, y que es necesario un mayor esfuerzo.

La V Encuesta Nacional sobre Seguridad Informática en Colombia (2005), realizada por la Asociación Colombiana de Ingenieros de Sistemas (ACIS) estudió las tendencias entre los años 2002-2005. Con la participación de 182 personas. Hacia 2008, ACIS presenta los resultados de la VIII Encuesta Nacional de Seguridad Informática, que ese año ascendió a 202 personas de los diferentes sectores productivos del país en el tema de seguridad de la información. Según el análisis comparativo (2002-2008), el 62,56% de las empresas tienen entre 1 a 5 personas dedicadas a Seguridad Informática, un 7,66% más que el año anterior; el 36,5% no cuenta con ningún tipo de certificación, un 23,8% menos que en 2007; Las certificaciones CISSP, CISA y CISM [2]son la más valoradas por el mercado y las que a la hora de considerar un proyecto de seguridad de la información marcan la diferencia para su desarrollo y contratación. En cuanto a políticas de seguridad, un 22,53% no las tienen

[2] CISSP es entregada por (ISC)2, una organización sin fines de lucro dedicada a aspectos de seguridad de la información y que ha provisto Certificaciones Internacionales a profesionales desde 1992. Certified Information Systems Auditor (CISA); Certified Information Security Manager (CISM).

definidas, y un 45,05% sostienen que se encuentran en desarrollo, lo que da un total alarmante de 67,58% de empresas sin políticas formalmente definidas (Cano J. J., Seguridad Informática en Colombia, tendencias 2008, 2008).

En 2009, la IX Encuesta Nacional de Seguridad Informática**,** con una participación de 222 personas, arroja conclusiones importantes: *"Las regulaciones nacionales e internacionales llevaran a las organizaciones en Colombia a fortalecer los sistemas de gestión de seguridad de la información; Estándares como ISO 27000, ITIL COBIT, y NIST*[3] *son los estándares de seguridad más usados para la gestión de la seguridad";* (Cano J. J., IX Jornada de Seguridad Informática, Monitoreo y Evolución de la Inseguridad Informática, 2009).

La X Encuesta Nacional sobre Seguridad Informática en Colombia (2010)**,** es la versión más reciente de este estudio, y presenta las tendencias futuras en el área de seguridad y el tema de interés del presente proyecto, las políticas de seguridad informática. Con una participación de 194 personas, los resultados reflejan la tendencia de inversión en seguridad centralizada en las redes y componentes, así como la protección a datos críticos. Aparece el tema de seguridad de la información como un elemento emergente que se empieza a imponer a nivel nacional.

Para este año, se presenta una disminución de la inversión en seguridad en la franja menor de los USD$50.000, pero se siguen presentando crecimientos importantes entre los USD$50.000 a $70.000, debido a la cantidad normativas y regulaciones alrededor de la industria nacional, que motiva la inversión en mayores recursos para la protección de la información.

Respecto a políticas de seguridad informática, el 16,5% de empresas no tienen medidas definidas; mientras el 49,69% responden que están actualmente en desarrollo, para una cifra inquietante del 66,19% sin políticas formalmente definidas, es decir, escritas,

[3] *Information Technology Infrastructure Library*, es el estándar en la Gestión de Servicios Tecnologías de Información. Tecnología . NIST por sus siglas en inglés, National Institute of Standards and Technology es una agencia de la Administración de Tecnología del Departamento de Comercio de los Estado Unidos.

documentadas, e informadas al personal. Lo que significa que las políticas informáticas requieren, aún, un alto grado de atención y esfuerzo conjunto entre la administración y el área de sistemas o tecnología de la organización, con el propósito de que la toma de decisiones desde el nivel superior sea coherente con las habituales y progresivas necesidades de seguridad en la información, redes y sistemas computacionales existentes (Junco, 2009).

En síntesis, actualmente se evidencia la necesidad de contar con políticas formalmente definidas como parte fundamental del Sistema de Gestión de Seguridad de la Información o esquema establecido. Sin embargo, el interés último está orientado hacia la continuidad de negocio, el cumplimiento de regulaciones y las normativas internas y externas, así como la protección de la reputación de la empresa, lo que proyecta un futuro de altas inversiones. Por otro lado se puede afirmar, según las encuestas nacionales, que las normas o regulaciones nacionales e internacionales fortalecerán los sistemas de gestión, dado el interés manifiesto (Junco, 2009).

En relación a la situación de inseguridad informática, en la región Caribe colombiana no se registran informes de proyectos orientados al establecimiento de modelos de seguridad de la información. A nivel nacional, se destaca el proyecto diseñado por el Grupo de Investigación en Informática y Telecomunicaciones de la Universidad Icesi de Cali/Colombia, que desarrolló un Centro de Operaciones de Seguridad Informática, cuyo objetivo es prestar servicios a empresas para las que es muy costoso tener personas y equipos especializados en la gestión de la seguridad informática. Lo interesante del proyecto es que facilita esa gestión a través del sistema SOC Colombia, una herramienta basada en OSSIM. La aplicación SOC Colombia fue un proyecto financiado por Colciencias[4] e Infivalle[5]. OSSIM (*Open Source Security Information Manager, o Administrador de la Seguridad de la Información de Fuente Abierta*) es un software que permite administrar, mantener y monitorear herramientas de seguridad como antivirus,

[4] Departamento Administrativo de Ciencia, Tecnología e Innovación. Promueve las políticas públicas para fomentar la Ciencia Tecnología e Innovación en Colombia.
[5] El Instituto Financiero para el Desarrollo del Valle del Cauca Infivalle, es un Establecimiento Público del Orden Departamental, descentralizado, de fomento y desarrollo regional.

detectores de intrusos, firewalls, analizadores de vulnerabilidades, monitores de red, sniffers etc. por lo que fue base fundamental para la construcción de SOC Colombia. El propósito del proyecto es ofrecer al encargado de la seguridad la capacidad de monitorear el estado de todos sus sistemas informáticos, desde una interfaz amigable. Es decir, deben existir políticas preestablecidas que incluyan estas actividades (Universia Noticias Colombia, 2009).

Adicionalmente, la Asociación Colombiana de Ingenieros de Sistemas publica que existen aproximadamente 60 empresas dedicadas actualmente a la seguridad informática en Colombia (Borghello C. F., Segu-Info, Seguridad de la Información, 2010). Sin embargo, el panorama actual indica que no han logrado mayor impacto en las organizaciones. Es decir, aunque el interés en el país es creciente, la temática de seguridad informática sigue estando relegada por otros elementos considerados de mayor relevancia. De acuerdo a un artículo publicado por el periódico el Tiempo en línea, es el caso de la mayoría de organizaciones del estado. Santos C, el autor, afirma "*No estoy seguro de cuál sea la entidad que tenga que ordenar el requerimiento de que las empresas estatales se homologuen en ISO 27001, estándar que especifica lo que se debe hacer para implementar y mantener un sistema de administración de la seguridad de la información, pero es algo que hay que llevar a cabo. Mientras tanto, valdría la pena evaluar cuáles son las políticas de seguridad informática implantadas en las entidades gubernamentales, para ver su eficiencia y cómo se administran y se obliga a utilizarlas*." (Calderón, 2010) Según sus afirmaciones, son pocas las empresas estatales que protegen sus activos físicos y lógicos, dejando en tela de juicio la seguridad informática del estado.

Desde esa perspectiva, tal vez, lo que hace falta no son entidades que brinden servicios de seguridad, sino, *crear conciencia* de los riesgos a los que están expuestos los sistemas de información crítica, y la *disposición de herramientas* que permitan dar los primeros pasos en la implantación de medidas de seguridad informática.

3. MARCO TEÓRICO

3.1. POLITICAS DE SEGURIDAD INFORMÁTICA Y ASPECTOS RELACIONADOS

El uso de las tecnologías de la información y las comunicaciones además de ser una ventaja para las organizaciones, en la actualidad representa una necesidad constante para superar fronteras y mantenerse competitivo. Esto ha obligado a concentrar esfuerzos en la búsqueda de mecanismos que permitan un adecuado aprovechamiento de los recursos informáticos y la protección de la información debido a múltiples problemas de seguridad presentados. La seguridad informática es un área que contribuye precisamente al logro de estos propósitos, su labor es proteger los recursos informáticos incluyendo la información almacenada en los sistemas e instalaciones, garantizando que se encuentren disponibles para el cumplimiento de sus funciones.

Algunos autores señalan que el *objetivo principal* de la seguridad informática se resume en aislar los actos no deseables y prevenir aquellos no contemplados aún o, lo que es igual, prevenir futuras pérdidas. En contraste, otros sostienen que es "*mantener la Integridad, Disponibilidad, Privacidad, Control y Autenticidad de la información manejada por computadora"* (Murillo, 2010).

Sin embargo, la conceptualización es un aspecto amplio en virtud de diferentes perspectivas. Lo realmente interesante es abordar el tema de seguridad en las organizaciones, lo cual implica la aplicación de métodos, reglas técnicas y/o actividades destinadas a proteger todo aquello que consideremos susceptible de robo, fraude, modificación, interceptación, daño o difusión indebida, dentro de la infraestructura informática.

Antes de tratar algunas de estas herramientas, es preciso mencionar otros aspectos representativos como los *elementos*, atendidos dentro de la seguridad informática, mediante su implementación (Borghello C. F., Seguridad Informática, sus implicancias e implementación, 2010): *Integridad*, Garantizar que los componentes del sistema no se

alteren indebidamente. *Disponibilidad,* Que el sistema esté disponible para los usuarios en cualquier momento. *Privacidad o confidencialidad,* Solo los usuarios autorizados pueden acceder al sistema. *Control,* Sólo el personal autorizado pueda decidir quién accede al sistema y qué información puede conocer. *Autenticidad,* Que la información requerida sea coherente en fondo y forma. *No repudio,* Control sobre las operaciones realizadas en el sistema, de tal forma que no se niegue la ejecución de una actividad. *Auditoría,* Que permita saber qué, cuándo, cómo y quién realizó acciones.

Cada uno representa un eslabón en la cadena *Seguridad Informática* que debe mantenerse fuerte en los gobiernos, las empresas, y otras organizaciones que desarrollan, poseen, proporcionan, administran servicios, y usan sistemas o redes de información (Ministerio de Administraciones Públicas, 2004). Adicionalmente, en el cumplimiento de los elementos se debe adquirir una serie de *compromisos específicos* de seguridad como No dificultar la labor de los usuarios, Responsabilizar a la gestión de riesgos de la seguridad, Especificar claramente las responsabilidades en seguridad, Definir una estructuración perceptible de la seguridad y que la protección tenga un costo aceptable (Murillo, 2010). Este conjunto de pautas están orientadas a cumplir con el propósito de dar una solución correcta al problema de inseguridad sin obstaculizar el flujo normal de los procesos internos y externos.

Teniendo en cuenta objetivos principales, elementos, y compromisos de la seguridad informática en condiciones tan cambiantes, a través de los tiempos se han construido marcos estratégicos de administración de la seguridad informática, con bases y resultados sólidos, dentro de los que se destacan los Sistemas de Gestión de Seguridad de la Información (SGSI).

Un SGSI se puede definir como el grupo de estrategias que engloban la gestión de la seguridad de la Información, considerando ésta el recurso más valioso para las organizaciones y el más vulnerable a la vez. Formalmente, según (Huerta, 2004) es un "*Sistema de gestión*[6] *que comprende la política, la estructura organizativa, los procedimientos, los procesos y los recursos necesarios para implantar la gestión de la*

[6]Establece e implementa los procesos que permiten a una organización realizar un producto o servicio de manera conforme a unas especificaciones dadas (CERINI, 2002).

seguridad de la información". Al respecto, las empresas deben lograr y mantener niveles de seguridad exigidos, para lo cual implementan tareas que lo garanticen; su realización comprende la denominada Gestión de la seguridad. De esta forma, la seguridad deja de ser un producto para asumirse como un *proceso* constante y complejo de controlar. Los SGSI o ISMS por sus siglas en inglés "Information Security Management System" tienen su origen en el estándar para la seguridad de la información ISO/IEC 27001 que establece etapas, elementos, hitos, propósitos y consecuentemente, un proceso claro para la administración organizada y confiable de la seguridad de la información.

Una de las etapas iniciales para implantar un SGSI consiste en identificar posibles fallas y vulnerabilidades actuales en los sistemas e infraestructura informática general, lo que permitirá determinar qué se debe proteger, cuándo, cómo y quién debe hacerlo, estableciendo posteriormente medidas al respecto que concienticen al personal de los problemas, los riesgos y la necesidad de afrontarlos, es decir, teniendo como precedente que los medios técnicos son insuficientes por sí mismos es necesario involucrar a toda la empresa. En el desarrollo del proceso especificado esta labor la cumple las **Políticas de Seguridad Informática (PSI)**, herramienta empleada en los Sistemas de Gestión de Seguridad con el propósito de concienciar a los miembros de las organizaciones mediante la definición de mecanismos y procedimientos que se deben adoptar para salvaguardar la información, junto a los procesos y sistemas que hacen uso de ella (CERINI, 2002).

De acuerdo a la figura 1, las políticas describen y representan los fundamentos de la seguridad, valiéndose de estándares y procedimientos para su implementación.

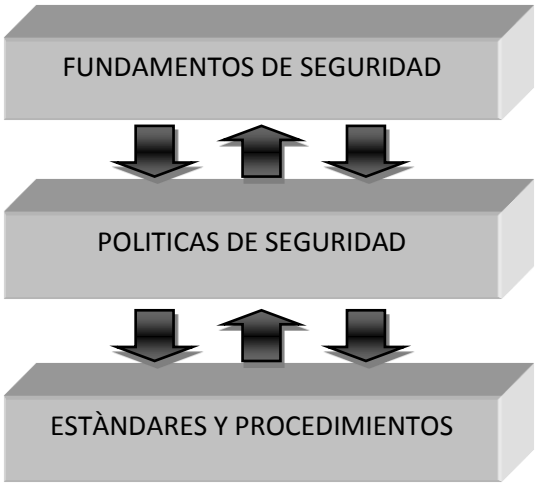


Figura 1. Relación entre estándares y políticas de seguridad. Tomada de (Amaya, 2004).

Técnicamente, han surgido diversos conceptos en relación a las PSI, *"Declaración de intenciones de alto nivel que cubre la seguridad de los sistemas informáticos y que proporciona las bases para definir y delimitar responsabilidades para las diversas actuaciones técnicas y organizativas que se requieran"* (Vieites, DIRECTRICES PARA LA DEFINICION E IMPLANTACION DE POLITICAS DE SEGURIDAD, 2009). *"Son una forma de comunicación con el personal, ya que las mismas constituyen un canal formal de actuación, en relación con los recursos y servicios informáticos de la organización. Estas a su vez establecen las reglas y procedimientos que regulan la forma en que una organización previene, protege y maneja los riesgos de diferentes daños"*.

Según (Howard, 2003) es una "*Declaración general de principios que presenta la posición de la administración para una área de control definida. Las políticas se elaboran con el fin de que tengan aplicación a largo plazo y guíen el desarrollo de reglas y criterios más específicos que aborden situaciones concretas. Las políticas son desplegadas y soportadas por estándares, mejores prácticas, procedimientos y guías*".

De acuerdo a esta última definición, se debe hacer claridad sobre los conceptos en los que se soportan las políticas de seguridad según (Howard, 2003), como sigue. Un Estándar es

una *"Regla que especifica una acción o respuesta que se debe seguir a una situación dada. Los estándares son orientaciones obligatorias que buscan hacer cumplir las políticas. Los estándares sirven como especificaciones para la implementación de las políticas: son diseñados para promover la implementación de las políticas de alto nivel de la organización antes que crear nuevas políticas".*

Mientras que una Mejor practica la define como "*una regla de seguridad específica a una plataforma que es aceptada a través de la industria al proporcionar el enfoque más efectivo a una implementación de seguridad concreta. Las mejores prácticas son establecidas para asegurar que las características de seguridad de sistemas utilizados con regularidad estén configurados y administrados de manera uniforme, garantizando un nivel consistente de seguridad a través de la organización."*

De igual modo, *"Una guía es una declaración general utilizada para recomendar o sugerir un enfoque para implementar políticas, estándares y buenas prácticas. Las guías son, esencialmente, recomendaciones que deben considerarse al implementar la seguridad. Aunque no son obligatorias, serán seguidas a menos que existan argumentos documentados y aprobados para no hacerlo."*

Siendo finalmente, los Procedimientos los que *"definen específicamente cómo las políticas, estándares, mejores prácticas y guías serán implementados en una situación dada. Los procedimientos son dependientes de la tecnología o de los procesos y se refieren a plataformas, aplicaciones o procesos específicos"*.

En síntesis, se puede hacer una analogía que permita diferenciarlos. Se requiere llegar de modo eficiente, práctico y eficaz a una meta que se encuentra en un lugar lejano, para ello existen muchos caminos conocidos o no. En este sentido, una política define, en principio, qué se debe hacer para un caso específico teniendo presente las condiciones del terreno, los estándares son orientaciones o patrones obligatorios que han sido desarrollados para hacer cumplir las políticas, una mejor práctica recoge la experiencia que han tenido otros al recorrer uno u otro camino llegando con éxito al final, una guía es un enfoque general que sugiere un camino a seguir para llegar a la meta señalando posibles elementos a utilizar,

mientras que los procedimientos definen cómo se implementarán las políticas, estándares, mejores prácticas y guías en ese caso. Es decir, dictan los pasos y actividades a realizar en una situación dada, mientras se recorre el camino.

De esta forma, las políticas de seguridad informática surgen como el fundamento principal en el logro de altos niveles de seguridad siendo soporte de la alta gerencia en la gestión de riesgos, integridad de los servicios críticos y en el uso adecuado de las tecnologías, plataformas y redes de telecomunicaciones. Se enmarcan en la protección de aquellos recursos considerados susceptibles de ataques que puedan afectar la información y por consiguiente la estabilidad, rentabilidad e imagen de la organización. De acuerdo a esto, para proteger la información en todo sentido han sido considerados dos enfoques o áreas de acción: Seguridad Física y Seguridad Lógica

La seguridad física de acuerdo a (Borghello C. F., Seguridad Informática, sus implicancias e implementación, 2010) consiste en la *"aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial"*, es decir, la seguridad a nivel físico pretende reducir los riesgos a los que se exponen los sistemas de cómputo e información, como piezas de la estructura informática de la compañía correspondientes al material crítico para su funcionamiento. De hecho, cualquier falla de este tipo puede acarrear que personajes interesados en causar daño, encuentren más fácil obtener un dato inicial base para culminar su proceso, por vía física.

En relación a esto, anteriormente se mencionó, dentro de los conceptos, que las PSI establecen reglas que regulan la forma en que una organización maneja riesgos no importando su origen. Algunos de los riesgos más prominentes e imprevisibles son los causados por la naturaleza y el ser humano, razón por la cual, se consideran diferentes tipos de desastres, teniendo en cuenta la prevalencia de unos sobre otros dependiendo de características propias de la empresa e instalación. Desde ese punto de vista las políticas de seguridad física están enfocadas principalmente a problemas relacionados con:

- Incendios, el fuego es uno de los principales enemigos de las computadoras, puede destruir archivos de información y programas.
- Inundaciones, es una de las causas de mayores desastres en centros de cómputo.
- Condiciones climatológicas, generalmente son avisadas anticipadamente (tormentas, tifones, sismos, entre otros).
- Señales de radar, pueden inferir en el procesamiento electrónico de la información, si la señal alcanzada por el computador es >= 5 Volt/Metro.
- Instalación eléctrica, la debe analizar un especialista que revise aspectos como picos y ruidos electromagnéticos, cableado (cableado de alto nivel de seguridad, pisos de placas extraíbles), sistema de aire acondicionado, emisiones electromagnéticas.
- Acciones hostiles como: *Robo,* la pérdida de una computadora ó el uso excedido del tiempo de máquina por parte del personal (fuera de sus labores), facilita la sustracción de información valiosa o confidencial así como software de uso exclusivo. *Fraude,* los equipos son utilizados con otros fines. Se presenta sustracción de altas cifras de dinero. *Sabotaje,* interferencia de las operaciones por acciones externas.
- Control de acceso, manejo del acceso controlando la identificación restricciones de tiempo, área o sector de la empresa. Implica la utilización de guardias, detectores de metales, sistemas biométricos, verificación automática de firmas.

En consecuencia se puede señalar que el control y seguimiento de la seguridad física es la base para la integración de un esquema de seguridad informática en la organización. En otras palabras, es imprescindible ubicar la seguridad física en un nivel importancia igual al de seguridad lógica de forma que se asegure la efectividad y aplicación de este último.

Correspondientemente la seguridad lógica es un tema delicado. Generalmente los daños o pérdidas no se presentan a causa de los problemas previstos, o en su defecto, los ataques no están destinados a medios físicos, sino a los sistemas software o información que éstos almacenan, indispensable en los procesos críticos. Por ello, Borghello precisa "*la*

seguridad lógica es la aplicación de barreras y procedimientos que resguarden el acceso a los datos y sólo se permita acceder a ellos a las personas autorizadas para hacerlo".

De acuerdo con esto, la seguridad lógica debe garantizar que todo aquello que no está permitido sea prohibido; es decir, tiene como objetivo proteger acceso a programas o archivos, evitar que se pueda modificar programas o datos sin autorización, garantizar que la información no se altere en la transmisión y mantener sistemas de respaldo.

Por lo tanto, consiste en resguardar el núcleo de los activos, que corresponde a datos e información de soporte, indispensable para la operación organizacional. El control de acceso, tanto interno como externo, es labor de ésta área. Siendo los delitos informáticos[7], el principal campo de acción de las PSI en la actualidad, con el propósito de contrarrestar los ataques a nivel lógico propiamente.

3.2. ETAPAS DE LAS POLITICAS DE SEGURIDAD INFORMÁTICA

El "ciclo de vida" de una política comprende 11 etapas que puede agruparse en cuatro fases, dependiendo de ciertos aspectos comunes. Como se muestra en la figura 2.

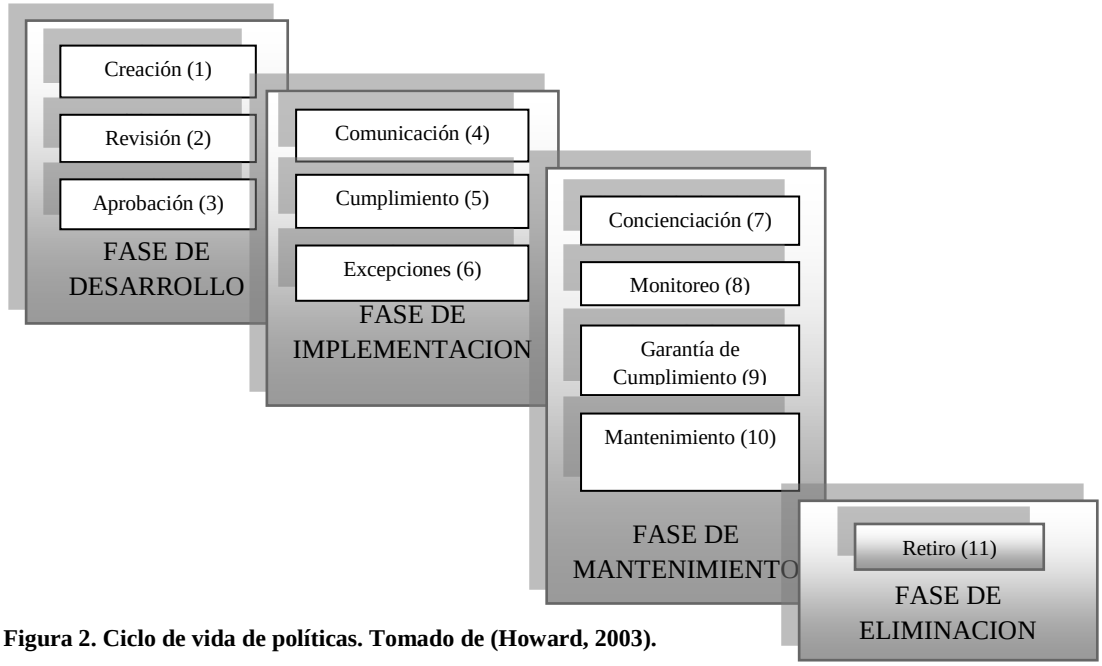


Figura 2. Ciclo de vida de políticas. Tomado de (Howard, 2003).

[7] Acciones antijurídicas o no autorizadas relacionadas con el uso de sistemas informáticos como medio para atentar contra la información (Borghello C. F., Seguridad Informática, sus implicancias e implementación, 2010).

En la primera fase, las políticas son creadas, revisadas y aprobadas, para que sean comunicadas y cumplidas a cabalidad, con ciertas excepciones necesarias, en la fase de Implementación. Se puede decir que en estas dos primeras fases las políticas de seguridad comienzan a marcar territorio en la organización; sin embargo, como el proceso de implantación de nuevas directrices, no es tarea fácil, más bien es un trabajo que requiere de mucha disciplina y compromiso por parte del personal, se contempla un tercer lapso en que se debe educar a los funcionarios o miembros de la empresa de la importancia de la seguridad de la información y el resguardo de los sistemas para su manejo, custodiar el cumplimiento de la política, además de actualizarla cuando se amerite.

3.2.1. FASE DE DESARROLLO

- **Creación**

La primera fase inicia consta de tres etapas. Como se observó en la figura 2, la creación de la política es la que marca el primer paso en el proceso (Howard, 2003).

Figura 3. Esquema de la etapa de creación de PSI. Fuente: Grupo de trabajo.

- **Revisión**

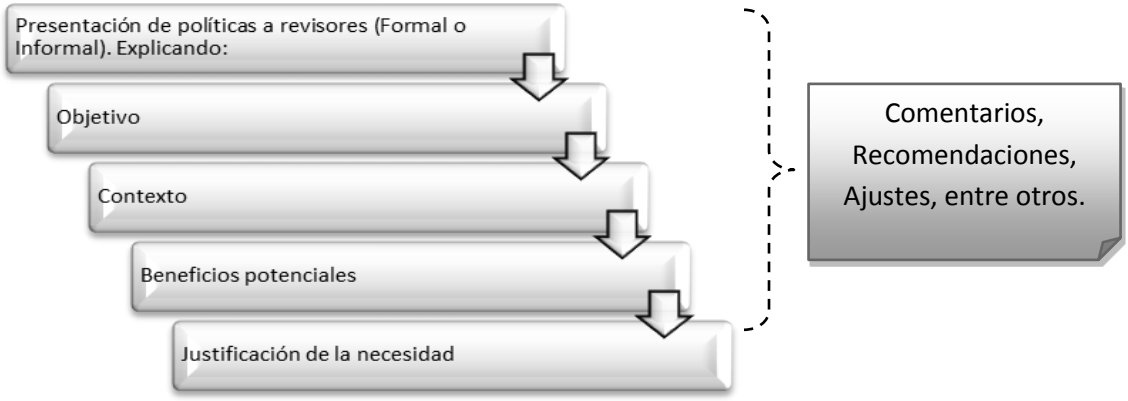


Figura 4. Elementos a considerar en la etapa de revisión. Fuente: Grupo de trabajo.

- **Aprobación**

El objetivo de esta etapa es obtener el aval de la administración y los entes involucrados en la dirección de la organización, para dar inicio a la implementación de la política, que es la fase siguiente del proceso.

3.2.2. FASE DE IMPLEMENTACION

Al llegar a la fase de implementación las políticas deben ser comunicadas inicialmente al personal; éste es un punto crucial para que el proceso arroje buenos resultados, porque es el recurso humano quién finalmente aplica las políticas (Howard, 2003).

- **Comunicación**

El siguiente diagrama la describe.

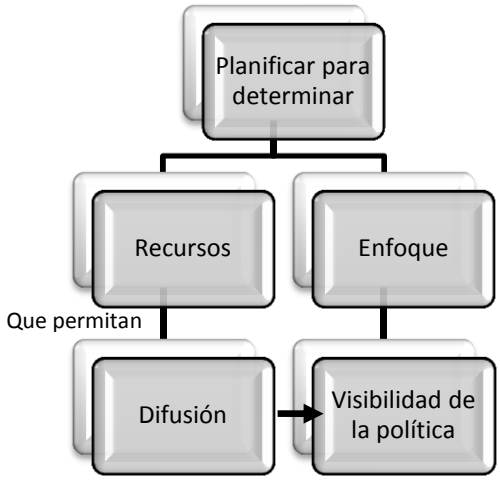


Figura 5. Esquema de la etapa de comunicación de políticas de seguridad informática. Fuente: Grupo de trabajo.

- **Cumplimiento**

Para dar cumplimiento a las políticas es necesario que la etapa de comunicación haya sido exitosa, o por lo menos, que actividades realizadas las hayan difundido adecuadamente (Howard, 2003). Por lo tanto, las acciones siguientes están orientadas hacia la ejecución, de manera que las personas interesadas e implicadas entiendan la política y su forma de aplicación ante diversas situaciones, eventos y áreas. El resultado de esta fase es un documento que informa el estado de la política.

- **Excepciones**

Debe establecerse u proceso para garantizar que las excepciones son registradas, analizadas, comunicadas y aprobadas o no.

3.2.3. FASE DE MANTENIMIENTO

Esta fase se puede sintetizar en el esquema ilustrado en la figura 6.

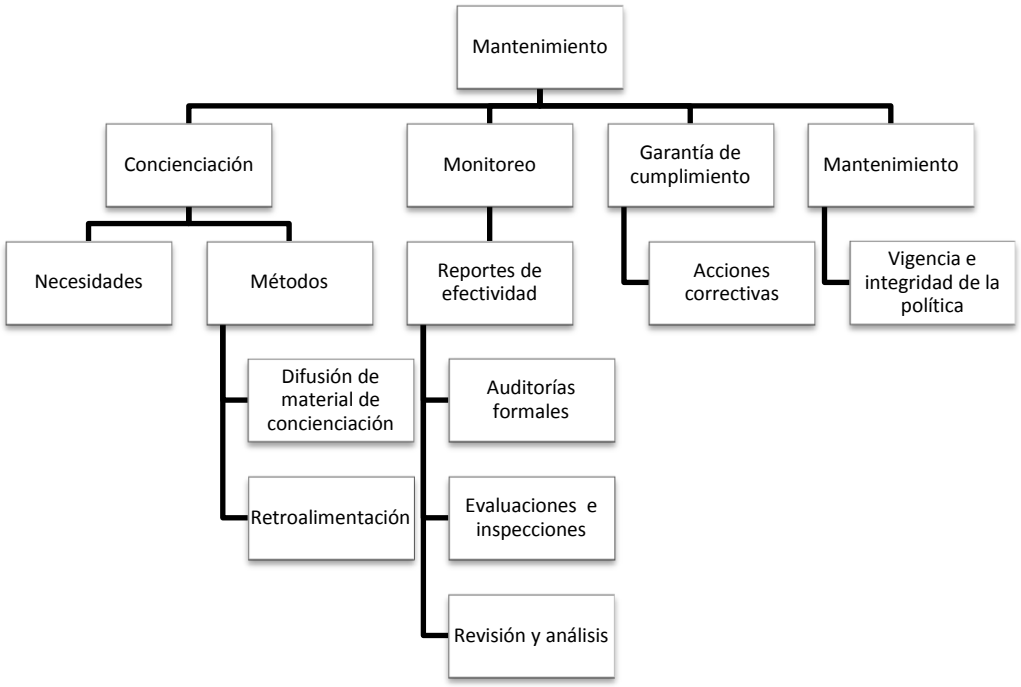


Figura 6. Esquema de la fase de mantenimiento de políticas de seguridad informática. Fuente: Grupo de trabajo, basado en (Howard, 2003).

3.2.4. FASE DE ELIMINACIÓN

- **Retiro**

En ésta última fase del ciclo de vida, cuando la política ha cumplido su ciclo y no es necesario seguir implementándola es mejor eliminarla o reemplazarla.

3.3. NORMAS Y ESTÁNDARES MÁS CONOCIDOS Y APLICADOS

Como se ha mencionado, el primer fundamento para la aplicación de políticas son los estándares o normas, a partir de éstos se obtiene una orientación hacia el cumplimiento de las mismas. Los estándares más conocidos y usados en la actualidad son:

- COBIT
- RFC2196
- TCSEC (Trusted Computer Security, militar, US, 1985).
- ITSEC (Information Technology Security, europeo, 1991).
- Common Criteria (internacional, 1986-1988).
- ISO/IEC 17799 (Basada en la BS 7799; 1) también llamada ISO 27002 (británico + internacional, 2000).
- ISO 27001 (Basada en 7799; 2)

Sin embargo, a partir de que ISO 17799 ha sido aceptado como estándar internacional, es el más desarrollado y aplicado en las organizaciones por brindar una guía de buenas prácticas de seguridad (Huerta, 2004). La adaptación española se denomina UNE- ISO/IEC 17799.

La norma UNE-ISO/IEC 17799 establece diez dominios de control que cubren por completo la Gestión de la Seguridad de la Información. De estos diez dominios se derivan 36 objetivos de control (resultados que se esperan alcanzar mediante la implementación de controles) y 127 controles (prácticas, procedimientos o mecanismos que reducen el nivel de riesgo). A pesar de tratarse de una norma NO CERTIFICABLE, recoge la relación de controles a aplicar (o al menos a evaluar) para establecer un Sistema de Gestión de Seguridad de la Información (SGSI) según la norma UNE- ISO/IEC 27001 (tiene su origen en UNE 71502, versión española CERTIFICABLE). Entre tanto, ISO-27001:2005 es el único estándar aceptado internacionalmente para la administración de la seguridad de la información y aplica a todo tipo de organizaciones, tanto por su tamaño como por su actividad. Se calculan aproximadamente 2800 empresas certificadas a nivel mundial (1800 en Japón, 415 en Reino Unido, 11 en Brasil, 3 en Argentina, etc.).

4. METODOLOGÍA

Teniendo en cuenta objetivos y características del proyecto, la investigación realizada se identifica de acuerdo a diferentes criterios: *Aplicada* según la utilidad que se pretende dar al conocimiento, debido a su interés en la aplicación, utilización y consecuencias prácticas de los conocimientos teóricos adquiridos; *Documental y de Laboratorio*, de acuerdo al lugar y fuentes de información, respectivamente; *Descriptiva y Analítica*, porque describe la temática estudiada a partir de características particulares que son analizadas con el fin de especificar propiedades importantes; además de ser una investigación *Vertical*, también denominada *Transversal*, conforme apunta su desarrollo a un momento y tiempo definido.

Las actividades que permitieron dar cumplimiento a cada uno de los objetivos específicos, orientados hacia el logro del objetivo general del proyecto, son las siguientes:

Diseño y aplicación de instrumentos de recolección de información. Posterior contacto y comunicación virtual con profesionales de Colombia y España, (Caixanova, EOSA y SIMCe Consultores), asesores en el proceso de investigación. Estudio de casos de aplicación de diferentes normas de apoyo a las políticas de seguridad en las organizaciones. Búsqueda y apropiación del conocimiento en estándares, normas, o modelos de gestión de Buenas Prácticas en Seguridad de la Información y Seguridad Física principalmente, destacando las normas internacionales ISO 17799, e ISO 27001. De esta forma, se creó un referente teórico que sirvió de base para la delimitación del proyecto y el desarrollo del Esquema de seguridad, Software y documentación a presentar.

Documental y de Laboratorio: *Inicialmente, se consultó sobre Seguridad Informática, políticas de seguridad física y lógica, normas, estándares internacionales, modelos o guías relacionadas; así mismo, se realizó una búsqueda sobre propuestas similares. Se realizó contacto virtual con el Dr. Álvaro Gómez Vieites, Asesor desde España, para la documentación y enfoque del proyecto. Seguidamente, se diseñaron los formatos de la encuesta de sondeo a organizaciones locales; y el de Observación no Estructurada, para ser diligenciados en empresas y por los integrantes del grupo de trabajo, respectivamente.*

Las conclusiones y resultados de estas técnicas de recolección de información revelaron fallas en la seguridad física que fueron de especial interés por los investigadores. A partir de estas investigaciones y asesorías recibidas, se estableció el enfoque del modelo de seguridad informática a construir, especificando la orientación hacia Políticas de Seguridad Informática a nivel de seguridad FÍSICA, como una parte del macroproyecto de investigación del programa de Ingeniería de Sistemas de Unicartagena.

Construcción de cuadros comparativos y evaluaciones detalladas, que evidencien los aspectos ventajosos de cada modelo, estándar y/o norma, y posterior clasificación y documentación de las estrategias claves encontradas, a fin de adaptarlas al esquema a construir.

Descriptiva: Delimitado el proyecto, se continuó con el estudio detallado de los estándares y normas seleccionadas; posteriormente, se establecieron criterios de comparación, que dieron lugar a cuadros de evaluación por estándar. De esta forma, se describieron aspectos y características destacadas y se continuó con su documentación.

Análisis de cuadros comparativos y estructuración de un Esquema de referencia, que proporcione una base común para la definición y desarrollo de normas de seguridad dentro de las empresas u organizaciones, que constituya una práctica eficaz de la gestión de la seguridad. Modelado del software, a través de herramientas I-CASE, y posterior proceso de desarrollo del mismo, siguiendo la metodología RUP. Esta aplicación, constituirá una serie de pasos por las diferentes etapas de creación e implantación de políticas de seguridad; su estructura será basada en el Esquema de referencia.

Descriptiva y Analítica: Una vez construidos los cuadros comparativos (que permitieron la evaluación de estándares), se realizó un proceso de análisis de bases de datos y estadísticas de estudios sobre el estado actual y tendencias del mercado en cuanto a incidentes de seguridad informática (específicamente en seguridad física) y la naturaleza de éstos, fundamentado en la teoría de la Dualidad, lo que permitió establecer necesidades y requerimientos reales, y extraer elementos de cada uno, para dar la estructura al modelo de seguridad. A la par, se estudiaron los estándares de seguridad física de centros de

cómputo y el ciclo de vida de las políticas, con la finalidad de proporcionar soporte a los lineamientos a sugerir en la creación de las políticas. En síntesis, se construye el Esquema de referencia de políticas de seguridad informática.

El paso siguiente fue el proceso de análisis y diseño del software, que materializa el esquema construido, a través de herramientas de modelado UML, y siguiendo la metodología RUP para desarrollar la aplicación.

Elaboración de documento donde se identifican los elementos básicos para el desarrollo de una estrategia de seguridad de la información, basado en las normas internacionales. Con el fin de brindar mejores fundamentos en la creación de políticas y procedimientos. Búsqueda e Implementación de mecanismos que permitan mostrar resultados obtenidos y socializar conocimientos.

Descriptiva: Con el modelo de Seguridad Informática, denominado también Esquema de Referencia, construido y desarrollado a través de la aplicación web, el grupo de trabajo complementó los aportes en documentación al trabajo de investigación, identificando la estrategia sugerida y fundamentos tenidos en cuenta. Lo que finalmente, permitió participar en eventos internacionales afines con la temática, para mostrar los resultados y conocimientos adquiridos.

Realización de prueba a una organización de carácter educativo, aplicando el esquema propuesto, en la definición de las PSI para el centro de informática, a través del uso de la herramienta software como apoyo y guía durante el proceso de creación, redacción, clasificación y registro de éstas. Presentación de un breve informe de la praxis.

Transversal y Aplicada: La fase final del proyecto consistió en la adecuación de un escenario de prueba del modelo de seguridad desarrollado, mediante el uso del Aplicativo en el proceso de creación de las primeras políticas de seguridad física para la empresa de prestación de servicios AKENDOS S.A.S. La aplicación del modelo en esta prueba se llevó a cabo para las fases más importantes del proceso, realizándose un breve informe de la misma.

5. DISEÑO DEL ESQUEMA O MODELO DE SEGURIDAD INFORMÁTICA ORIENTADO HACIA POLÍTICAS DE SEGURIDAD FÍSICA

Este capítulo corresponde a la ejecución del proyecto investigativo; presenta la recolección de información realizada a través de diferentes técnicas, que dan paso a la Delimitación del proyecto. Luego, se estudian los estándares internacionales seleccionados mediante criterios establecidos. La sección siguiente, reúne análisis y fundamentos (estadísticos y teóricos) usados como criterios para la comparación de los estándares que fueron estudiados, y la selección de elementos que darán lugar al Esquema básico de seguridad. Seguidamente, el ítem 5.5 relaciona el estudio de estándares de seguridad física en centro de cómputo, como parte final para la estructuración del modelo en la sección 5.6 del capítulo.

5.1. RECOLECCIÓN DE INFORMACIÓN

En esta sección se presenta la información recopilada a través de las TRI (técnicas de recolección de información) aplicadas en la etapa de documentación y apropiación de conceptos, estándares y demás.

5.1.1. ANÁLISIS DE CONTENIDO: ESTUDIO DE ESTÁNDARES Y/O NORMAS SELECCIONADAS

De acuerdo a lo indicado en la sección 3.3 del Marco teórico, en relación a los estándares, a continuación se presenta el resultado del análisis de contenido realizado desde diferentes fuentes, como son: artículos publicados, ponencias publicadas, informes, reportes estadísticos, libros, documentos de páginas web, consultas a asesores, entre otros.

5.1.1.1. ISO 27001

Ha sido preparado con la finalidad de proporcionar un modelo para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI). Es decir, especifica los requerimientos para establecer ese sistema de gestión y la implementación de Controles de seguridad personalizados para las necesidades de las organizaciones individuales o partes de ella.

El diseño e implementación del SGSI de una organización es influenciado por las necesidades y objetivos, requerimientos de seguridad, los procesos empleados y el tamaño y estructura de la organización.

ENFOQUE DEL PROCESO

La aplicación de un sistema de procesos dentro de una organización, junto con la identificación y las interacciones de estos procesos, y su gestión, puede considerarse un 'enfoque del proceso'.

Un enfoque del proceso para la gestión de la seguridad de la información presentado en este Estándar Internacional fomenta que sus usuarios enfaticen la importancia de:

a. Entender los requerimientos de seguridad de la información de una organización y la necesidad de establecer una política y objetivos para la seguridad de la información;
b. Implementar y operar controles para manejar los riesgos de la seguridad de la información;
c. Monitorear y revisar el desempeño y la efectividad del SGSI; y
d. Mejoramiento continuo en base a la medición del objetivo.

ISO 27001 adopta el modelo del proceso Planear-Hacer-Chequear-Actuar (PDCA). Como se ilustra en la figura 7.

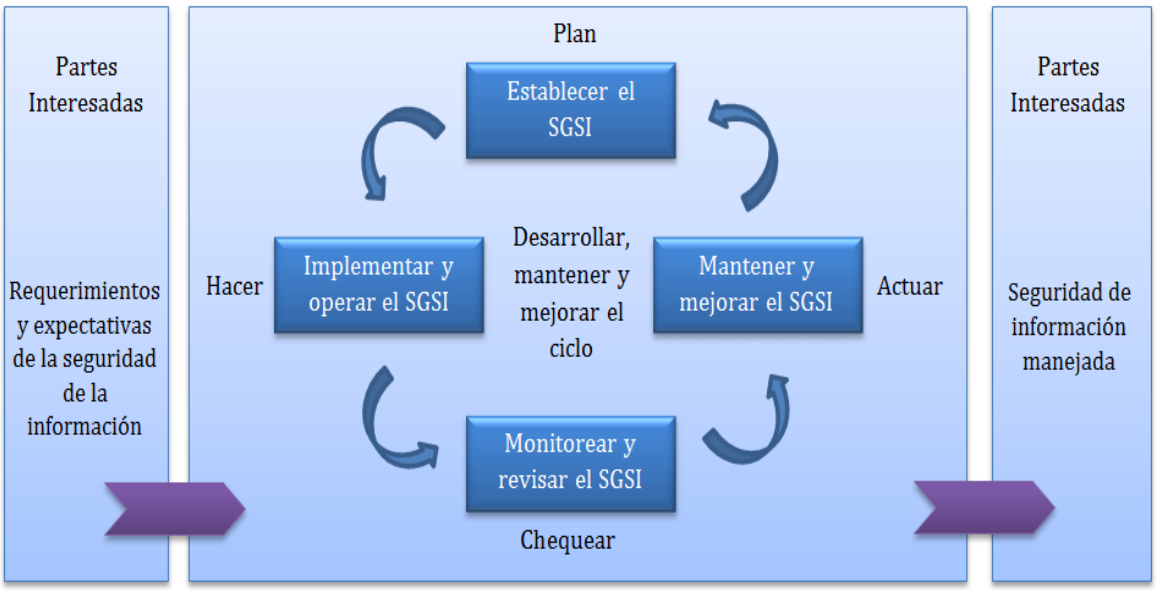


Figura 7. Modelo de proceso PDCA aplicado por el estándar a los procesos SGSI. Fuente: (Estándar Internacional ISO/IEC 27001, 2005).

Este Estándar Internacional está diseñado para permitir que una organización se alinee o integre su SGSI con los requerimientos del sistema de gestión relacionado. Abarcando todos los tipos de organizaciones (por ejemplo; empresas comerciales, agencias gubernamentales, organizaciones sin fines de lucro).

PROCESO PROPUESTO

1. Establecer el SGSI
2. Implementar y operar el SGSI
3. Monitorear y revisar el SGSI
4. Mantener y mejorar el SGSI

Por otro lado, es importante mencionar que la gerencia debe proporcionar evidencia de su compromiso en el establecimiento, implementación, operación, monitoreo, revisión, mantenimiento y mejoramiento del SGSI. Así mismo, la organización debe proveer los recursos necesarios y asegurar que todo el personal al que se le asignó responsabilidades definidas en el SGSI sea competente para realizar las tareas.

El documento original del presente estándar contiene los anexos correspondientes a los objetivos de control y controles propuestos.

5.1.1.2. ISO 17799

Establece los lineamientos y principios generales para iniciar, implementar, mantener y mejorar la gestión de la seguridad de la información en una organización. Los objetivos delineados en este Estándar Internacional proporcionan un lineamiento general sobre los objetivos de gestión de seguridad de la información generalmente aceptados.

Los objetivos de control y los controles de este Estándar Internacional son diseñados para ser implementados para satisfacer los requerimientos identificados por una evaluación del riesgo. Puede servir como un lineamiento práctico para desarrollar estándares de seguridad organizacional y prácticas de gestión de seguridad efectivas y para ayudar a elaborar la confianza en las actividades inter-organizacionales.

Los requerimientos de seguridad se identifican mediante una evaluación metódica de los riesgos de seguridad. El gasto en controles debiera ser equilibrado con el daño comercial probable resultado de fallas en la seguridad.

EVALUACIÓN DE LOS RIESGOS DE SEGURIDAD

Las evaluaciones del riesgo debieran identificar, cuantificar y priorizar los riesgos en comparación con el criterio para la aceptación del riesgo y los objetivos relevantes para la organización. Los resultados debieran guiar y determinar la acción de gestión apropiada y las prioridades para manejar los riesgos de la seguridad de la información y para implementar los controles seleccionados para protegerse contra estos riesgos. Es posible que el proceso de evaluación de riesgos y la selección de controles se deba realizar un número de veces para abarcar las diferentes partes de la organización o sistemas de información individuales.

ENFOQUE SISTÉMICO

La evaluación del riesgo debiera incluir el enfoque sistemático de calcular la magnitud de los riesgos (análisis del riesgo) y el proceso de comparar los riesgos estimados con un criterio de riesgo para determinar la importancia de los riesgos (evaluación del riesgo).

ESTRUCTURA DEL ESTÁNDAR

Este estándar contiene 11 cláusulas de control de seguridad conteniendo colectivamente un total de 39 categorías de seguridad principales y una cláusula introductoria que presenta la evaluación y tratamiento del riesgo.

CLÁUSULAS

Cada cláusula contiene un número de categorías de seguridad principales. Las once cláusulas (acompañadas por el número de categorías de seguridad principales incluidas dentro de cada cláusula) son:

a. Política de Seguridad (1);
b. Organización de la Seguridad de la Información (2);

c. Gestión de Activos (2);
d. Seguridad de Recursos Humanos (3);
e. Seguridad Física y Ambiental (2);
f. Gestión de Comunicaciones y Operaciones (10);
g. Control de Acceso (7);
h. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información (6);
i. Gestión de Incidentes de Seguridad de la Información (2);
j. Gestión de la Continuidad Comercial (1);
k. Conformidad (3).

5.1.1.3. COBIT

Las empresas exitosas reconocen los beneficios de la tecnología de información y la utilizan para impulsar el valor de sus interesados (*stakeholders*).

También entienden y administran los riesgos asociados, tales como el aumento en requerimientos regulatorios, así como la dependencia crítica de muchos procesos de negocio en Tecnologías de Información, referidas como **TI**, más adelante.

La necesidad del aseguramiento del valor de TI, la administración de los riesgos asociados a TI, así como el incremento de requerimientos para controlar la información, se entienden ahora como elementos clave del gobierno de la empresa. El valor, el riesgo y el control constituyen la esencia del gobierno de TI.

El gobierno de TI integra e institucionaliza las buenas prácticas para garantizar que la TI de la empresa sirva como base a los objetivos del negocio. De esta manera, el gobierno de TI facilita que la empresa aproveche al máximo su información.

- Maximizando así los beneficios,
- capitalizando las oportunidades y
- ganando ventajas competitivas

Para ello requiere: MARCO DE REFERENCIA (de trabajo) DE CONTROL de la TI.

Los Objetivos de Control para la Información y la Tecnología relacionada (COBIT) brindan **buenas prácticas** a través de un marco de trabajo de dominios y procesos, y presenta las actividades en una estructura manejable y lógica. Las buenas prácticas de COBIT representan el consenso de los expertos. Están enfocadas fuertemente en el control y menos en la ejecución. Estas prácticas ayudarán a optimizar las inversiones facilitadas por la TI, asegurarán la entrega del servicio y brindarán una medida contra la cual juzgar cuando las cosas no vayan bien.

La orientación al negocio que enfoca COBIT consiste en vincular las metas de negocio con las metas de TI brindando métricas y modelos de madurez para medir sus logros, e identificando las responsabilidades asociadas de los propietarios de los procesos de negocio y de TI. El enfoque hacia procesos de COBIT se ilustra con un modelo de procesos, el cual subdivide TI en 34 procesos de acuerdo a las áreas de responsabilidad de planear, construir, ejecutar y monitorear (Institute, 2005).

¿Cómo puede la empresa poner bajo control la TI de tal manera que genere la información que la empresa necesita? ¿Cómo puede administrar los riesgos y asegurar los recursos de TI de los cuales depende tanto? ¿Cómo puede la empresa asegurar que TI logre sus objetivos y soporte los del negocio?

1. Objetivos de control que definan la última meta de implantar políticas, procedimientos, prácticas y estructuras organizacionales
2. ¿Qué se debe medir y cómo? Medición objetiva.

La evaluación de la capacidad de los procesos basada en los modelos de madurez de COBIT es una parte clave de la implementación del gobierno de TI.

COBIT da soporte al gobierno de Tecnologías de Información al brindar un marco de trabajo que garantiza diferentes aspectos (figura 8).

Figura 8. Áreas focales del Gobierno de TI. Fuente: Grupo de Trabajo basado en (Institute, 2005).

Estas áreas focales de gobierno de TI describen los tópicos en los que la dirección ejecutiva requiere poner atención para gobernar la TI en sus empresas. La dirección operacional usa procesos para organizar y administrar las actividades cotidianas de TI. COBIT brinda un modelo de procesos genéricos que representa todos los procesos que normalmente se encuentran en las funciones de TI, ofreciendo un modelo de referencia común entendible para los gerentes operacionales de IT y del negocio. Se establecieron equivalencias entre los modelos de procesos COBIT y las áreas focales del gobierno de TI, ofreciendo así un puente entre lo que los gerentes operacionales deben realizar y lo que los ejecutivos desean gobernar. (Institute, 2005)

Debido a que COBIT se enfoca en el que se requiere para lograr una administración y control adecuados de TI, se posiciona a un alto nivel. Los más detallados estándares y las mejores prácticas de COBIT se encuentran a un bajo nivel de detalle describiendo cómo administrar y controlar aspectos específicos de TI. COBIT actúa como un integrador de

estos diferentes materiales guía, resumiendo los objetivos clave bajo un solo marco de trabajo que también liga los requisitos de gobierno y del negocio.

5.1.1.4. COMMON CRITERIA

Common Criteria es el resultado final de importantes esfuerzos en el desarrollo de **criterios de evaluación unificados** para la seguridad de los productos IT (Information Technology) y ampliamente aceptado por la comunidad internacional.

A principios de los años 80, se desarrollaron en Estados Unidos los criterios de seguridad recogidos bajo el nombre de TCSEC (Trusted Computer System Evaluation Criteria) y editados en el famoso "libro naranja". En las décadas posteriores, varios países tomaron como base el TCSEC americano y evolucionaron las especificaciones para hacerlas más flexibles y adaptables a la constante evolución de los sistemas de IT.

De ahí la comisión europea, en el año 1.991 publicó el ITSEC (Information Technology Security Evaluation Criteria), desarrollado conjuntamente por Francia, Alemania, Holanda y el Reino Unido. En Canadá, igualmente se desarrollaron en 1.993 los criterios CTCPEC (Canadian Trusted Computer Product Evaluation) uniendo los criterios americanos y europeos. En ese mismo año el Gobierno americano publicó los Federal Criteria como una aproximación a unificar los criterios europeos y americanos.

La culminación del proceso se dio tiempo después cuando la ISO estableció Common Criteria como estándar, constituyéndolo como ISO 15408 con el título de "Evaluation Criteria for Information Technology Security" (ISO/IEC 15408).

En la presente investigación se estudió el estándar genérico ISO/IEC 15408 (a continuación) y dos de las variaciones más importantes: ITSEC (Adaptación EE.UU y TCSEC Europea). Esto con la finalidad de rescatar características que puedan ser útiles para el esquema a construir.

ISO/IEC 15408 (CRITERIOS COMUNES)

La Norma internacional ISO 15408, también conocida como "Common Criteria" establece unos criterios de evaluación y certificación de la seguridad en Tecnologías de la Información. Quedan fuera de su marco de normalización los siguientes aspectos:

- Medidas administrativas
- Medidas físicas
- Marco legal de la evaluación
- Calidad intrínseca de los algoritmos de cifrado

JUSTIFICACIÓN

Muchos sistemas y productos de Tecnologías de la Información están diseñados para satisfacer y realizar tareas específicas y puede ocurrir, normalmente por razones económicas, que determinados aspectos de seguridad se encuentren delegados en funciones de seguridad de otros productos o sistemas de propósito general sobre los cuales ellos trabajan como pueden ser sistemas operativos, componentes software de propósito específico o plataformas hardware.

Por tanto, las medidas de salvaguarda dependen del correcto diseño y funcionamiento de los servicios de seguridad que implementan otros sistemas o productos IT más genéricos. Sería deseable por tanto, que éstos estuvieran sometidos a evaluación para conocer en qué medida nos ofrecen garantías y podemos depositar confianza en ellos. Muchos clientes y consumidores de sistemas y productos IT carecen de los conocimientos necesarios o recursos suficientes para juzgar por ellos mismos si la confianza que depositan en estos sistemas o productos IT es adecuada y desearían no obtener esa certeza solamente en base a la información que proporcionan los fabricantes o las especificaciones de los desarrolladores.

La norma ISO/IEC 15408 define un criterio estándar a usar como base para la evaluación de las propiedades y características de seguridad de determinado producto o sistema IT. Ello permite la equiparación entre los resultados de diferentes e independientes

evaluaciones, al proporcionar un marco común con el que determinar los niveles de seguridad y confianza que implementa un determinado producto en base al conjunto de requisitos de seguridad y garantía que satisface respecto a esta norma obteniendo de esa forma una certificación oficial de nivel de seguridad que satisface.

Por tanto, la norma ISO/IEC 15408 proporciona una guía muy útil a diferentes perfiles relacionados con las tecnologías de la seguridad. *Desarrolladores* de productos o sistemas de tecnologías de la información (fabricantes).Pueden ajustar sus diseños y explicar lo que ofrecen. Los *evaluadores* de seguridad, que juzgan y certifican en qué medida se ajustan una especificación de un producto o sistema IT a los requisitos de seguridad deseados. Es decir, puede certificar lo que asegura. Los *usuarios* que pueden conocer el nivel de confianza y seguridad que los productos de tecnologías de la información y sistemas le ofrecen y puede explicar lo que quiere.

1. Los usuarios pueden comparar sus requerimientos específicos frente a los estándares de Common Criteria para determinar el nivel de seguridad que necesitan.
2. Los usuarios pueden determinar más fácilmente cuando un producto cumple una serie de requisitos. Igualmente, Common Criteria exige a los fabricantes de los productos certificados publicar una documentación exhaustiva sobre la seguridad de los productos evaluados.
3. Los usuarios pueden tener plena confianza en las evaluaciones de Common Criteria por no ser realizadas por el vendedor, sino por laboratorios independientes. La evaluación de Common Criteria es cada vez más utilizada como condición necesaria para concurrir a concursos públicos. Por ejemplo, el Departamento de Defensa Americano ha anunciado planes para utilizar exclusivamente productos certificados por Common Criteria.
4. Debido a que Common Criteria es un estándar Internacional, proporciona un conjunto común de estándares que los usuarios con operaciones internacionales pueden utilizar para escoger productos que se ajusten localmente a las necesidades de seguridad.

En definitiva, proporcionando un conjunto de estándares en seguridad como los recogidos por Common Criteria, se crea un lenguaje común entre los fabricantes y los usuarios, que

ambos pueden entender. Los fabricantes utilizarán este lenguaje para contar a sus clientes potenciales las características de sus productos evaluadas en Common Criteria, e igualmente habilita a los usuarios a identificar y comunicar adecuadamente sus necesidades de seguridad. Se proporcionan unos medios y mecanismos objetivos que nos permitirán tomar decisiones en base algo más sólido que las meras percepciones.

PARTES DEL ESTÁNDAR

El ISO/IEC 15408 se presenta como un conjunto de tres partes diferentes pero relacionadas. A continuación, describimos cada una de ellas:

Parte 1. Introducción y modelo general. IS 154081: 1999(2002) Introduction and general model

Define los principios y conceptos generales de la evaluación de la seguridad en tecnologías de la información y presenta el modelo general de evaluación. También establece cómo se pueden realizar especificaciones formales de sistemas o productos IT atendiendo a los aspectos de seguridad de la información y su tratamiento. (La estructura y lenguaje comunes para expresar los requisitos de seguridad de productos o sistemas de TI).

- PP, protection profile (perfil de protección): lo que se quiere: requisitos para una categoría de productos
- ST, security target (objetivo de seguridad): fabricante: lo que ofreceré: especificaciones de un producto
- TOE , target of evaluation (objetivo de evaluación): una implementación de ST

Parte 2. Requisitos Funcionales de Seguridad IS 154082: 1999(2002) Security functional requirements

Este tipo de requisitos definen un comportamiento deseado en materia de seguridad de un determinado producto o sistema IT.

Parte 3. Requisitos de Garantías de Seguridad IS 154083: 1999(2002) Security assurance requirements

Este tipo de requisitos establecen los niveles de confianza que ofrecen funciones de seguridad del producto o sistema. Trata de evaluar qué garantías proporciona el producto o sistema en base a los requisitos que se satisfacen a lo largo del ciclo de vida del producto o sistema.

NIVELES DE GARANTÍA

Common Criteria o ISO/IEC 15408, proporcionan también unos niveles de garantía (EAL) como resultado final de la evaluación. EAL –Evaluated Assurance Level:

- EAL0: sin garantías
- EAL1: probado funcionalmente
- EAL2: probado estructuralmente
- EAL3: probado y chequeado metódicamente
- EAL4: diseñado, probado y revisado metódicamente
- EAL5: diseño y pruebas semiformales
- EAL6: diseñado, probado y verificado semiformalmente
- EAL7: diseñado, probado y verificado formalmente Constituyen la base para el reconocimiento mutuo

ORGANIZACIÓN DE LOS REQUISITOS DE SEGURIDAD

Los CC establecen unos criterios de evaluación basados en un análisis riguroso del producto o sistema IT a evaluar y los requisitos que este satisface. Para ello, establece una clasificación jerárquica de los requisitos de seguridad. Se determinan diferentes tipos de agrupaciones de los requisitos siendo sus principales tipos los que vemos a continuación:

- Clase: Conjunto de familias comparten un mismo objetivo de seguridad.
- Familia: un grupo de componentes que comparten objetivos de seguridad pero con diferente énfasis o rigor.
- Componente: un pequeño grupo de requisitos muy específicos y detallados. Es el menor elemento seleccionable para incluir en los documentos de perfiles de protección (PP) y especificación de objetivos de seguridad (ST).

5.1.1.5. ITSEC

Los criterios para la evaluación de la corrección distingue entre los criterios relativos a la forma en que el TOE[8] se desarrolla (construcción) y los criterios sobre la forma en que se utilizará (en funcionamiento). Para cada nivel de evaluación, los criterios de evaluación se desglosan en las diferentes fases y aspectos.

Para cada aspecto o fase, la documentación que debe presentarse para el examen ha sido identificado, seguido de los requisitos de su contenido y presentación, o de los procedimientos y normas que deben definir, seguido por las pruebas necesarias para demostrar que los criterios en cuestión se han cumplido y, finalmente, las acciones a ser realizadas por el evaluador se presentan.

Para mayor claridad, ya que existen requisitos muy diferentes para cada nivel de evaluación, los criterios para cada nivel se presentan por separado. Criterios nuevos o modificados en cada nivel están impresos en negrita. Hay una necesidad general de un mayor rigor y profundidad en las pruebas aportadas en los niveles más altos de evaluación. Esto se refleja en el uso progresivo del estado de los verbos, describir y explicar en los diferentes niveles de muchos criterios para el contenido y presentación que de otra forma no cambia.

MODELO DEL PROCESO

La evaluación de la exactitud determina si la seguridad de aplicación de las funciones y los mecanismos se aplica correctamente. Siete niveles de evaluación marcados E0 a E6 se han definido, en representación de niveles ascendentes de la confianza en la exactitud. E0 representa la confianza adecuada. E1 representa un punto de entrada por debajo del cual puede haber confianza útil cabo, y E6 representa el más alto nivel de confianza. Los niveles restantes representan una interpolación en el medio. La exactitud se aborda desde el punto de vista de la construcción de la TOE, que abarca tanto el proceso de desarrollo y el entorno de desarrollo, y también el punto de vista de funcionamiento de la TOE.

SISTEMAS DE GESTIÓN

[8] Utilizado para referirse a un producto o sistema a evaluar.

Gran parte del trabajo se ha hecho anteriormente en el desarrollo de TI criterios de evaluación de seguridad, aunque los objetivos ligeramente diferentes de acuerdo a las necesidades específicas de los países o los organismos involucrados. Lo más importante de ellos, y un precursor de otros desarrollos, en muchos aspectos, fue el equipo de Trusted Computer System Evaluation Criteria, comúnmente conocido como el TCSEC o "Libro Naranja", publicados y utilizados para la evaluación del producto por el Departamento de Defensa de EE.UU. Otros países, principalmente europeos, también tienen una importante experiencia en la evaluación de seguridad de TI y han desarrollado sus propios criterios de seguridad de TI. En el Reino Unido incluye CESG Memorándum número 3, desarrollado para el uso del gobierno, y las propuestas del Ministerio de Comercio e Industria, el "Libro Verde", para los productos comerciales de seguridad de TI. En Alemania, la Agencia de Información de Seguridad Alemana publicó una primera versión de sus propios criterios en 1989, y al mismo tiempo, los criterios se están desarrollando en Francia, los llamados "Blue-White-Red Book".

En vista de que el trabajo que estaba pasando en esta área, y todavía quedaba mucho por hacer, Francia, Alemania, Países Bajos y el Reino Unido reconoció que este trabajo necesario para ser abordado de manera concertada, y que armonizada común, Criterios de seguridad de TI debe ser presentado. Hay tres razones para la armonización:

a) Experiencia que es mucho lo que ha acumulado en los distintos países, y habría mucho que ganar de manera conjunta sobre la base de esa experiencia;

b) La industria no quería que diferentes criterios de seguridad en los diferentes países;

c) Los conceptos y enfoques básicos son los mismos, en todos los países e incluso en las aplicaciones comerciales, gubernamentales y de defensa.

Una serie de ejemplo de clases funcionales se han definido para corresponden de cerca a los requisitos de funcionalidad de las clases C1 TCSEC a A1. Se incluyen, como F-C1 F-B3. No es posible, sin embargo, relacionar los niveles de evaluación directamente a los requisitos de confidencialidad de las clases TCSEC, ya que los niveles ITSEC han sido

desarrollado por la armonización de los diferentes criterios de seguridad TI en Europa los regímenes que contienen una serie de requisitos que no aparecen en TCSEC explícitamente.

La intensión de correspondencia entre estos criterios y las clases TCSEC está de siguiente manera:

These Criteria	TCSEC clases
E0	D
F-C1, E1	C1
F-C2, E2	C2
F-B1, E3	B1
F-B2, E4	B2
F-B3, E5	B3
F-B3, E6	A1

Tabla 1. Correspondencia entre criterios y clases. Fuente: Grupo de Trabajo.

Cabe señalar que no hay funcionalidad de la clase F-A1 como los requisitos de funcionalidad de la clase A1 TCSEC son los mismos que para la clase B3. Un producto que ha sido diseñado con el objetivo de una evaluación exitosa contra ambos el ITSEC y TCSEC, y que se ha demostrado que cumple con una de las clases o las combinaciones en la tabla anterior, deben pasar la evaluación con los criterios de otros en la clase equivalente o una combinación. Sin embargo, en la C1 TCSEC requiere prueba que deberá presentar las pruebas del sistema de desarrollo. Así, un [F-C1, E1] evaluación sólo sería equivalente a la evaluación C1 si el promotor había elegido para cumplir el requisito opcional E1 para proporcionar la documentación de prueba como evidencia de las pruebas suficientes en contra del objetivo de seguridad antes de la evaluación.

5.1.1.6. TCSEC - Trusted Computer System Evaluation Criteria (libro naranja)

Objetivo: Aplicar la política de seguridad del Departamento de Defensa estadounidense. Esta política se preocupa fundamentalmente del mantenimiento de la confidencialidad de la información clasificada a nivel nacional.

Definen siete conjuntos de criterios de evaluación denominados clases:

D, C1, C2, B1, B2, B3 y A1 (clases) -> Política de seguridad, imputabilidad, aseguramiento y documentación (aspectos de evaluación). Funcionalidad y confianza.

El TCSEC definido en este documento clasifica los sistemas en cuatro grandes divisiones jerárquicas de la protección de la seguridad reforzada.

Sirven de base para la evaluación de la eficacia de los controles de seguridad integrados en los productos de procesamiento automático de datos del sistema. La evaluación de la eficacia técnica de seguridad informática.

Los criterios fueron desarrollados con tres objetivos:

a) Proporcionar a los usuarios un punto de referencia que permitan evaluar el grado de confianza que se puede colocar en los sistemas informáticos para el procesamiento seguro de la información clasificada o de otro tipo,
b) Proporcionar orientación a los fabricantes en cuanto qué construir en su nueva, ampliamente confiable y disponible línea de productos comerciales con el fin de satisfacer los requisitos para las aplicaciones sensibles, y
c) Proporcionar una base para la especificación de los requisitos de seguridad en las especificaciones de la adquisición.

ALCANCE

TCSEC definido en este documento aplica principalmente a la confianza de sistemas de procesamiento automático de datos (ADP) disponibles en el mercado. También son aplicables a la evaluación de los sistemas existentes y la especificación de requisitos de seguridad para la adquisición de sistemas de ADP.

1. los requisitos específicos de función de seguridad
2. los requisitos de garantía.

PROPÓSITOS

1. Proporcionar un estándar a los fabricantes en cuanto a qué características de seguridad construir en sus nuevos y previstos productos comerciales con el fin de proporcionar sistemas ampliamente disponibles que cumplan con los requisitos de confianza (con especial énfasis en la prevención de la divulgación de datos) para aplicaciones sensibles.
2. Proporcionar componentes del Departamento de Defensa con una métrica con la cual evaluar el grado de confianza que se puede colocar en los sistemas informáticos para el procesamiento seguro de la información clasificada y otros.
3. Proporcionar una base para la especificación de los requisitos de seguridad en las especificaciones de la adquisición.
4. En lo que respecta a la segunda propuesta para el desarrollo de los criterios, es decir, el suministro de componentes del Departamento de Defensa con una métrica de evaluación de seguridad, las evaluaciones pueden dividirse en dos tipos: (a) una evaluación se puede realizar en un producto informático desde una perspectiva que excluye la aplicación medio ambiente, o, (b) que se puede hacer para evaluar si las medidas de seguridad adecuadas se han tomado para permitir que el sistema sea usado en la práctica en un entorno específico.

Este último tipo de evaluación, es decir, las que se realizan con el propósito de evaluar los atributos de un sistema de seguridad con respecto a una misión operacional específica, que se conoce como una evaluación de la certificación. Debe entenderse que la realización de una evaluación formal del producto no constituye la certificación o acreditación del sistema para ser utilizado en cualquier entorno de aplicación específico. Por el contrario, el informe de evaluación sólo proporciona índice de confianza de un sistema informático de evaluación junto con el apoyo de datos que describe los puntos fuertes del sistema de productos y los puntos débiles desde el punto de vista de la seguridad informática. La

certificación de la seguridad del sistema y el procedimiento formal de aprobación/acreditación, realizado de acuerdo con las políticas de los organismos emisores, todavía deben ser seguidos antes de que un sistema pueda ser aprobado para su uso en la elaboración o manipulación de la información clasificada.

REQUISITOS FUNDAMENTALES DE SEGURIDAD INFORMÁTICA

Cualquier discusión sobre seguridad informática necesariamente parte de una exposición de las necesidades, es decir, lo que realmente significa para llamar a un sistema informático "seguro". En general, los sistemas seguros se controlarán, a través del uso de características de seguridad específicas, de tal manera que sólo las personas debidamente autorizadas tengan acceso a la información, o los procesos que operan en su nombre, tendrá acceso a leer, escribir, crear o borrar información. Seis requisitos fundamentales se derivan de esta declaración básica de objetivos: cuatro tratan de lo que se necesita siempre para controlar el acceso a la información, y dos tratan de cómo se puede obtener garantías creíbles de que esto se logra en un sistema informático de confianza.

POLÍTICA

Requisito 1. POLÍTICA DE SEGURIDAD - Debe existir una política de seguridad explícita y bien definida impuesta por el sistema. Teniendo en cuenta los sujetos y los objetos identificados, debe haber un conjunto de reglas que son utilizados por el sistema para determinar si a un determinado sujeto se puede permitir tener acceso a un objeto específico. Los sistemas informáticos de interés deben aplicar una política de seguridad obligatoria que puedan aplicar eficazmente las reglas de acceso para el manejo sensible (por ejemplo, clasificar) la información. Estas normas incluyen requisitos tales como: Ninguna persona que carece de permiso adecuado del personal de seguridad podrá acceder a información clasificada. Además, los controles discrecionales de seguridad son necesarios para garantizar que sólo determinados usuarios o grupos de usuarios pueden obtener acceso a los datos (por ejemplo, basados en la necesidad de saber).

Requisito 2. MARCADO - las etiquetas de control de acceso deben estar asociadas a los objetos. Con el fin de controlar el acceso a la información almacenada en una computadora, de acuerdo con las reglas de una política de seguridad obligatoria, debe ser posible para marcar cada objeto con una etiqueta que identifique realmente el nivel de sensibilidad del objeto (por ejemplo, clasificación), y/o los modos de acceso otorgado a los individuos que potencialmente puede tener acceso al objeto.

RESPONSABILIDAD

Requisito 3. IDENTIFICACIÓN – los individuos deben ser identificados. Cada acceso a la información debe ser mediada sobre la base de quién está accediendo a la información y qué clase de información está autorizado a tratar. Esta información de identificación y autorización debe estar bien asegurada por el sistema informático y asociada con cada uno de los elementos activos que realizan alguna acción de seguridad relevante en el sistema.

Requisito 4. RESPONSABILIDAD - La información de auditoría debe ser guardada y protegida de forma selectiva a fin de que las acciones que afectan la seguridad se puedan remontar a la parte responsable. Un sistema de confianza debe ser capaz de registrar la ocurrencia de eventos relevantes para la seguridad en un registro de auditoría. La capacidad de seleccionar los eventos de auditoría a ser registrados es necesaria para reducir al mínimo los gastos de auditoría y para permitir un análisis eficiente. Los datos de auditoría deben ser protegidos contra la modificación y destrucción no autorizada para permitir la detección e investigación de posteriores hechos y violaciones de seguridad.

GARANTÍA

Requisito 5. SEGURIDAD - El sistema informático debe contener mecanismos de hardware/software que puedan ser evaluados independientemente para ofrecer garantías suficientes de que el sistema aplica los requisitos de 1 a 4 anteriores. Con el fin de asegurar que los cuatro requisitos de Política de Seguridad, Señalización, identificación, y rendición de cuentas son soportados por un sistema informático, debe haber alguna colección

identificada y unificada de los controles de hardware y software que realizan esas funciones. Estos mecanismos son típicamente integrados en el sistema operativo y están diseñados para llevar a cabo las tareas asignadas de manera segura. La base para confiar en los mecanismos de tal sistema en su entorno operativo debe estar claramente documentado de tal manera que es posible examinar de forma independiente los datos para evaluar su suficiencia.

Requisito 6. PROTECCIÓN CONTINUA - Los mecanismos de confianza que cumplen estos requisitos básicos deben ser siempre protegidos contra la manipulación y / o cambios no autorizados. Ningún sistema informático puede ser considerado realmente seguro si el hardware y software básico y los mecanismos que hacen cumplir la política de seguridad también están sujetos a modificaciones no autorizadas o la subversión. El requisito de protección continua tiene implicaciones directas en todo el ciclo de vida del sistema de computadora. Estos requisitos fundamentales son la base para la aplicación de criterios de evaluación individual para cada división de la evaluación y la clase.

5.1.1.7. RFC 2196

Esta guía está dirigida a proporcionar una orientación básica en el desarrollo de un plan de seguridad para su sitio. Un enfoque generalmente aceptado a seguir es el propuesto por (Fites & Kratz, 1989), e incluye los siguientes pasos:

a) Identificar qué objeto se está intentando proteger
b) Identificar de qué se está tratando de proteger al objeto
c) Determinar cuáles son las probables amenazas
d) Implementar medidas que protegerán los bienes, medidas en costo/eficiencia
e) Revisar el proceso continuamente y efectuar las correcciones cada vez que se detecte un problema

EVALUACIÓN DE RIESGOS

Una de las razones más importantes para crear una política de seguridad es que el gasto efectuado en ello produce beneficios en el costo de no tenerla. Aunque esto parezca obvio, es posible confundirse acerca de dónde se debe enfocar el esfuerzo. Como ejemplo, existe

gran cantidad de publicidad acerca de los intrusos en computación, pero los estudios de seguridad computacional muestran que en la mayoría de las organizaciones, la pérdida de confianza en las personas es mucho mayor en la actualidad.

El análisis de riesgo involucra la determinación de qué es lo que se necesita proteger, de qué protegerlo y cómo protegerlo. Este es el proceso de determinar todos los riesgos, organizándolos por nivel de gravedad. Esto involucra tomar decisiones desde el punto de vista costo/beneficio, en relación con lo que se quiere proteger. Como se mencionó anteriormente, no se debe gastar en proteger algo, más allá de su valor.

En relación al análisis de riesgo, existen dos elementos que se tratarán:

a) Identificar los bienes
b) Identificar las amenazas

Para cada bien, los objetivos básicos de seguridad son: disponibilidad, confiabilidad e integridad. Para ello, cada amenaza debe ser analizada en función de su efecto en estos objetivos.

Identificación de los bienes

El primer paso en el análisis de riesgo es identificar todo aquello que debe ser protegido. Algunos son obvios, como el valor de la propiedad de la información, la propiedad intelectual y los elementos de hardware, pero algunos no son considerados, como las personas que operan los sistemas. El punto esencial es listar todas aquellas cosas que podrían ser afectadas por un problema de seguridad.

Una lista de categorías es sugerida por *Pfleeger* (Pfleeger, 2003), la cual considera:

a) Hardware: CPU, teclados, terminales, workstations, computadores personales, impresoras, unidades de discos, líneas de comunicación, servidores y equipos de comunicaciones.
b) Software: Programas fuente, programas objeto, utilitarios, programas de diagnóstico, sistemas operativos, programas de comunicaciones.
c) Datos: En ejecución, almacenados en línea, archivados off-line, backups, registros de auditorías, bases de datos, en tránsito sobre medios de comunicación.
d) Personas: Usuarios, administradores, mantenedores de hardware.

e) Documentación: De programas, hardware, sistemas, procedimientos administrativos locales.
f) Suministros: Papel, formularios, cintas, medios magnéticos.

Identificación de las amenazas

Una vez que se identifican los elementos que requieren protección, es preciso identificar las amenazas hacia ellos. En seguida se analizan las amenazas, para determinar los potenciales daños que existen. Esto ayuda a identificar de qué amenazas se está intentando proteger los elementos. Las siguientes son amenazas clásicas que deben ser consideradas. Dependiendo de la situación, habrá más amenazas específicas que identificar y localizar:

- Acceso no autorizado a recursos y/o información
- Revelación involuntaria o no autorizada de información
- Denegación de servicio

5.1.2. OBSERVACIÓN NO ESTRUCTURADA

La observación no estructurada (participante) es un tipo de observación en la cual el investigador tiene, como propósito principal, lograr un conocimiento exploratorio y aproximado de un fenómeno, en vez de tratar de comprobar alguna hipótesis. A través de este recurso, se obtuvieron referentes de la situación real en algunos ambientes empresariales respecto al manejo de Políticas de Seguridad Informática, con la finalidad de anotar características particulares a tener en cuenta en el diseño del esquema de seguridad informática. A continuación se ilustran los formatos diseñados con los datos encontrados.

FORMATO PARA LA APLICACIÓN DE OBSERVACION NO ESTRUCTURADA O PARTICIPANTE

Datos generales			
NOMBRE DEL OBSERVADOR:		Yessica Julie Marrugo Marrugo	
Tiempo de observación:	4 meses	Sector Organización:	Servicios
Rol dentro de la organización:		Auxiliar de Sistemas	

Demografía	
¿Cuántos empleados, calcula que tiene la organización?	180

¿Cuántos de ellos, pudo notar, conocen el tema de seguridad informática?		40
¿Observó errores humanos que pusieran en riesgo la integridad de información crítica?	SI	NO
	X	
Fallas de seguridad y control de acceso		
¿Notó la existencia de controles que detecten posibles fallas de seguridad?	SI	NO
		X
¿Existe un mecanismo de identificación y autenticación?	X	
¿Está basado en el uso de contraseñas?	X	
¿Existe un procedimiento de cambio de contraseñas?	X	
¿El uso de contraseñas y su resguardo es controlado debidamente? (observó casos de contraseñas escritas en el escritorio, pegadas en el monitor…)		X
¿Con que frecuencia observó la ocurrencia de incidentes de seguridad?	Semanal	
Herramientas y prácticas de seguridad física		
¿Se hace algún tipo de revisión del sistema de información de forma periódica?	SI	NO
		X
¿Observó filtros y estabilizadores eléctricos en la red eléctrica de suministro a los equipos?	X	
¿Observó Sistemas de Alimentación Ininterrumpida?	X	
¿Existe algún control que impida el acceso físico a los recursos a personal no autorizado? (puertas de seguridad, alarmas, tarjetas de acceso)		X
¿Existe algún mecanismo físico que impida el uso no autorizado de sistemas de información?		X
Políticas de Seguridad		

¿Conoció de la existencia de alguna política de seguridad global en la empresa?		X
¿Conoció un(os) responsable(s) de coordinar las medidas de seguridad aplicables?		X
¿Le dieron a conocer algún plan de contingencia?		X
¿Se dispone de personal informático involucrado directamente con la seguridad del sistema?		X

Comentarios adicionales (Señale anécdotas o casos de incidentes, fallas u omisiones que presenció, puede anotar cualquier comentario que considere no se tuvo en cuenta en el cuestionario anterior).

Anécdota : En una ocasión el jefe inmediato se retrasó, y el día anterior había realizado el cambio de contraseña del sistema de información manejado (cumpliendo con la política de cambio de contraseña de la empresa), entonces mi obligación era empezar a trabajar y que los procesos no se entorpecieran; el problema era que no conocía la nueva clave de acceso; sin embargo, me acerqué al escritorio y levanté por curiosidad un calendario de notas, y observé algo que pensé podía ser, al digitarlo en el sistema me di cuenta que efectivamente era la contraseña de acceso a la base de datos, que entre otras cosas contiene toda la información crítica del área en cuestión.

Entre otras fallas, observé constantes caídas de los servidores, lo que provocaba cese casi total de las actividades de la empresa.

Falta de conciencia de los miembros de la organización.

Recomendaciones (Mencione sugerencias o pautas que considere se deben tener en cuenta en la organización)	Concienciar al personal de la importancia de la seguridad informática en organización Diseñar e implementar políticas de seguridad acordes con las necesidades empresariales. Empezar por la creación de las políticas de seguridad física en la empresa, que incluye el recurso humano.
Conclusiones (Debe plantear su punto de vista con base en la observación que realizó,	Según la observación, considero que aunque la empresa está organizacionalmente bien estructurada y cuenta con personal calificado, se desconocen aspectos, como la implantación de seguridad informática, que actualmente

haciendo una síntesis de los aspectos de seguridad física que considere se deben fortalecer en la organización)	pueden determinar su continuidad, pues su funcionamiento depende de los datos generados a diario, lo que implica que cualquier perdida o manipulación inadecuada de la información influye negativa y representativamente en la prestación de servicios, es decir, en el flujo normal de los procesos. En este sentido, se sugiere implantar medidas de seguridad física orientadas al adecuado manejo de los sistemas por parte del personal; así como controles de acceso físicos a las instalaciones, equipos y sistemas, y medidas técnicas para proteger la infraestructura computacional.

FORMATO PARA LA APLICACIÓN DE OBSERVACION NO ESTRUCTURADA O PARTICIPANTE

Datos generales			
NOMBRE DEL OBSERVADOR:		Ronald Nuñez Barcos	
Tiempo de observación:	6 meses	Sector Organización:	Servicios
Rol dentro de la organización:		Desarrollador Web	

Demografía		
¿Cuántos empleados, calcula que tiene la organización?		9
¿Cuántos de ellos, pudo notar, conocen el tema de seguridad informática?		7
¿Observó errores humanos que pusieran en riesgo la integridad de información crítica?	SI	NO
	X	

Fallas de seguridad y control de acceso		
¿Notó la existencia de controles que detecten posibles fallas de seguridad?	SI	NO
		X
¿Existe un mecanismo de identificación y autenticación?	X	
¿Está basado en el uso de contraseñas?	X	
¿Existe un procedimiento de cambio de contraseñas?		X
¿El uso de contraseñas y su resguardo es controlado debidamente? (observó casos de contraseñas escritas en el escritorio, pegadas en	X	

el monitor…)		
¿Con que frecuencia observó la ocurrencia de incidentes de seguridad?	Semanal	
Herramientas y prácticas de seguridad física		
¿Se hace algún tipo de revisión del sistema de información de forma periódica?	SI	NO
		X
¿Observó filtros y estabilizadores eléctricos en la red eléctrica de suministro a los equipos?	X	
¿Observó Sistemas de Alimentación Ininterrumpida?	X	
¿Existe algún control que impida el acceso físico a los recursos a personal no autorizado? (puertas de seguridad, alarmas, tarjetas de acceso)		X
¿Existe algún mecanismo físico que impida el uso no autorizado de sistemas de información?		X
Políticas de Seguridad		
¿Conoció de la existencia de alguna política de seguridad global en la empresa?		X
¿Conoció un(os) responsable(s) de coordinar las medidas de seguridad aplicables?		X
¿Le dieron a conocer algún plan de contingencia?		X
¿Se dispone de personal informático involucrado directamente con la seguridad del sistema?		X
Comentarios adicionales (Señale anécdotas o casos de incidentes, fallas u omisiones que presenció, puede anotar cualquier comentario que considere no se tuvo en cuenta en el cuestionario anterior). Anécdota: En una ocasión uno de los empleado y socio de la empresa tuvo una pérdida de información por un virus que ataco su portátil ya que no contaba con un antivirus instalado, debido a que decía que el ese tipo de cosas no le pasa ya que hasta ese momento no había tenía un incidente tan grave como el de perder información valiosa desde entonces decidió instalar un antivirus que lo protegiera.		

Entre otras fallas, pude observar constantes caídas del servicio de internet, lo que provocaba cese parcial de las actividades de la empresa.	
Recomendaciones (Mencione sugerencias o pautas que considere se deben tener en cuenta en la organización)	Concienciar al personal de la importancia de la seguridad informática en organización Diseñar e implementar políticas de seguridad que aborden las necesidades empresariales enfocadas hacia la seguridad física.
Conclusiones (Debe plantear su punto de vista con base en la observación que realizó, haciendo una síntesis de los aspectos de seguridad física que considere se deben fortalecer en la organización)	A pesar de ser una empresa dedicada al desarrollo de aplicaciones web y de contar con personal calificado, sus esquemas de seguridad son precarios en cuanto a la política de claves y el control de acceso de los diferentes servicios que utiliza, en cuanto a la continuidad de la operación cuenta con UPS que si bien mitigan el problema no es una solución eficaz en cuanto al tiempo que logra suplir las necesidades de la empresa, otro problema observado es el de la intermitencia del servicio de internet, todo esto atenta con la continuidad del negocio. Según la observación, se sugiere implantar políticas de seguridad física pensada en afrontar los problemas que presenta la empresa con el fin de controlar los incidentes que puedan afectar el desempeño de su proceso productivo, como por ejemplo controles de acceso a los equipos así como a los diferentes servicios que utiliza, capacitar al personal para que se cree la conciencia sobre la amenazas que se pueden presentar.

Figura 9. Imágenes de la aplicación de Observación No estructurada; a) Observación en empresa número 1. b) Observación en empresa número 2. Fuente: Grupo de Trabajo.

A partir de la observación ilustrada en la imagen a) se puede indicar lo siguiente:

- Se evidencia el desconocimiento de los empleados en relación al tema de seguridad informática en general.
- El personal interno está involucrado en los incidentes observados.
- Faltan controles de detección de fallas.

- La existencia de autenticación e identificación en los sistemas no ha sido garantía de protección.
- Existen medidas físicas de protección a los sistemas de cómputo, sin embargo, la falta de controles de acceso físico a los recursos puede hacer que éstas no sean efectivas.
- No hay Políticas de seguridad formalmente definidas, sólo algunas normas internas.
- Algunas fallas de seguridad física observadas que aparentemente son de poco impacto, pueden resultar graves, hasta el punto de atentar contra la integridad de la información crítica.

De la experiencia y observación mostrada en la imagen b) se destaca:

- A pesar que la mayoría del personal tiene conocimiento en el área informática no se presta la atención debida a las políticas de seguridad.
- Existen medidas que mitigan fallas frecuentes de energía, sin embargo, éstas son sólo parciales debido a que no dan una solución eficaz.
- No hay políticas de seguridad formalmente definidas.
- Frecuentes caídas en el servicio de internet lo que interfieren en el funcionamiento de la empresa.
- El acceso a los diferentes servicios se hace bajo una misma dupla usuario/clave lo que imposibilita llevar un registro de eventos.
- Además, estos servicios pueden ser accedidos desde fuera de la red privada de la compañía, lo que la hace vulnerables a ataques.
- No existe un sistema de control de acceso físico a los diferentes servicios y componentes de la organización.

5.1.3. ENCUESTA (SONDEO)

Esta sección comprende los resultados de la encuesta de sondeo realizada a empresas locales (Cartagena, Colombia).

UNIVERSIDAD DE CARTAGENA

Programa Ingeniería de Sistemas
Facultad de Ingeniería 60 años

Encuesta de soporte para el proyecto de grado titulado: **Software de Apoyo al proceso de creación y registro de Políticas de Seguridad Informática en organizaciones.**

Objetivo: Determinar la existencia de políticas de seguridad informática e identificar posibles inconvenientes para su implementación.

Empresa:	Nombre de encuestado:		
	Cargo:		
Según el ámbito de la actividad, su organización se clasifica como:		Local	
		Regional	
		Nacional	
		Multinacional	
¿A qué sector pertenece la organización?		Extractivas	
		Servicios	
		Comercial	

Figura 10. Ilustración de encuesta realizada.

Con un total de 15 empresas de servicio encuestadas, los resultados muestran que el 93% de éstas no tiene un área de seguridad informática dentro de la estructura organizacional; el restante 7% tienen una persona dedicada exclusivamente a la temática. Así mismo, el 40% de las empresas manifiesta haber invertido en tecnologías de seguridad informática los últimos 2 años.

La totalidad de los encuestados afirma tener presente la posibilidad de ser víctima de ataques hacia su información. Además, el 40% de los negocios presencian incidentes de seguridad (virus, caídas del sistema, pérdida de datos…) semanalmente; 40% quincenalmente y el 20% restante, mensualmente. Sin embargo, sólo un 20% cuenta con una política formalmente definida (ver figura 11). Además, el 13% responde haber conocido algún esquema de seguridad que fue aplicado a la organización, mientras el 87% no conocen ninguno.

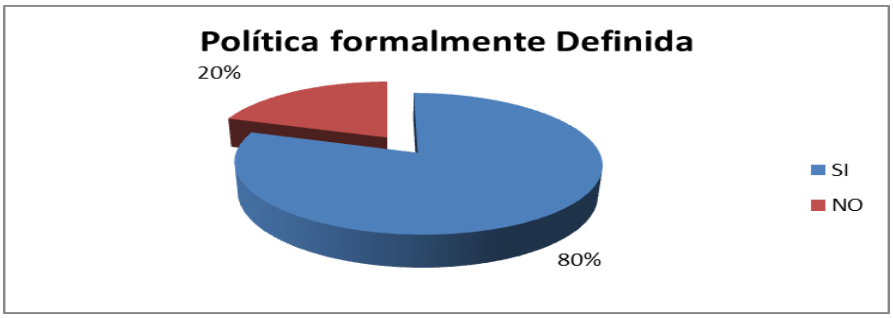


Figura 11. Empresas con políticas formalmente definidas. Fuente: Grupo de Trabajo.

Uno de los datos más llamativos es que el 100% de las empresas locales partícipes no posee ninguna certificación en seguridad informática. A su vez el 47% dice haber contemplado proyectos orientados a la seguridad de sus activos. Lo que es coherente con la disposición de invertir en seguridad, que mostraron el total de éstas.

Respecto a los estándares o buenas prácticas de seguridad, un 67% dice identificar alguno. Como ilustra la figura 12, la encuesta indica que ISO 27001 es el más conocido.

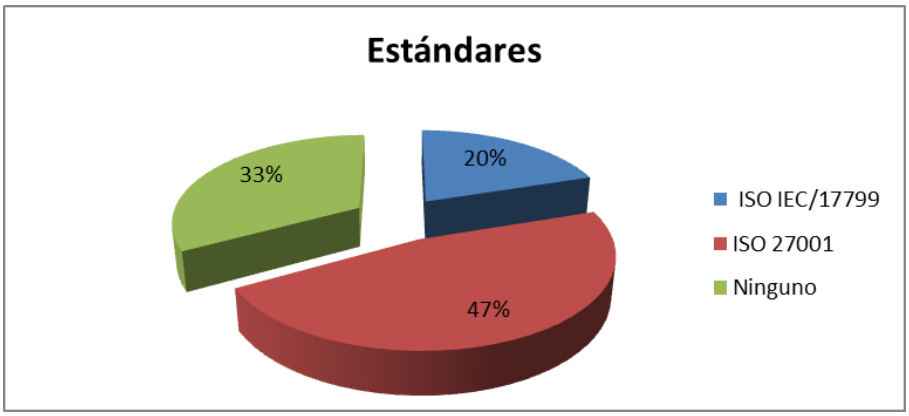


Figura 12 . Estándares identificados por encuestados. Fuente: Grupo de Trabajo.

Adicionalmente, a la pregunta sobre qué impacto tendría para la organización certificarse en alguno de estos estándares, el 80% sostiene la continuidad del negocio; lo que indica que a pesar de que el nivel de seguridad en las empresas en reducido, existe conciencia sobre el beneficio de implantar este elemento. El gráfico permite observar que el aumento de credibilidad es también un factor importante en algunas empresas.

Figura 13. Impacto de certificación en estándares. Fuente: Grupo de Trabajo.

La figura 14 es un buen indicador de viabilidad para proyectos orientados hacia el apoyo software en el proceso de creación de políticas de seguridad en las empresas, pues indica que el 87% de los encuestados considera el *software guía* como una buena alternativa para empezar a implantar seguridad informática en las empresas, mediante el desarrollo de medidas.

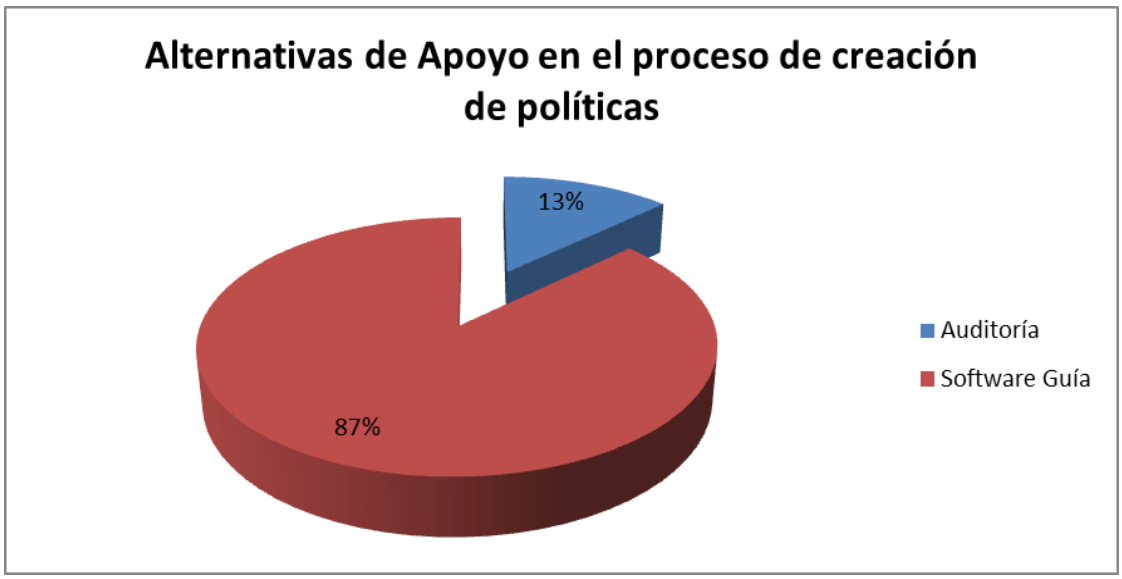


Figura 14. Herramientas de apoyo en el proceso de creación de políticas de seguridad informática. Fuente: Grupo de Trabajo.

Los datos aportados por la encuesta permiten discernir sobre la necesidad de implantar estrategias de seguridad informática en las empresas, debido a los constantes incidentes, y falta de mecanismos que los prevengan o reduzcan. La importancia de este elemento para la continuidad del negocio es innegable, por lo tanto, el crecimiento de la economía local y nacional puede verse seriamente afectado en cualquier momento, si no se toman las respectivas medidas.

Adicionalmente, la disposición de invertir, la identificación de estándares de seguridad aplicados, como ISO/IEC 17799 e ISO 27001, y la conciencia de que existen fallas en la organización que ponen en riesgo los activos, son buenos precedentes para desarrollar herramientas que sean de ayuda y orientación para las empresas en estos aspectos; teniendo

como indicador el auge de los procesos sistematizados, y la opinión de las empresas respecto a las alternativas mostradas.

5.2. DELIMITACIÓN DEL PROYECTO

Como se estudió en la sección 3.1 del Marco teórico, la Seguridad Informática aborda cuatro elementos fundamentales en las organizaciones: datos, software, hardware y personas; los cuales pueden ser agrupados en dos enfoques o áreas de acción: Seguridad Lógica y Seguridad física, tal como se ilustra en la figura 15. De esta forma, a través de políticas de seguridad, los datos, el software, el hardware y las personas son salvaguardados y relacionados dentro de un marco general de seguridad informática que busca determinar qué se quiere proteger, de qué y cómo protegerlo. En este sentido, investigadores del Programa de Ingeniería de Sistemas de la Universidad de Cartagena plantearon el desarrollo de un Macro proyecto que aborde esta área desde dos grupos de trabajo (Seguridad Lógica y Seguridad Física) que presenten alternativas de solución al problema identificado.

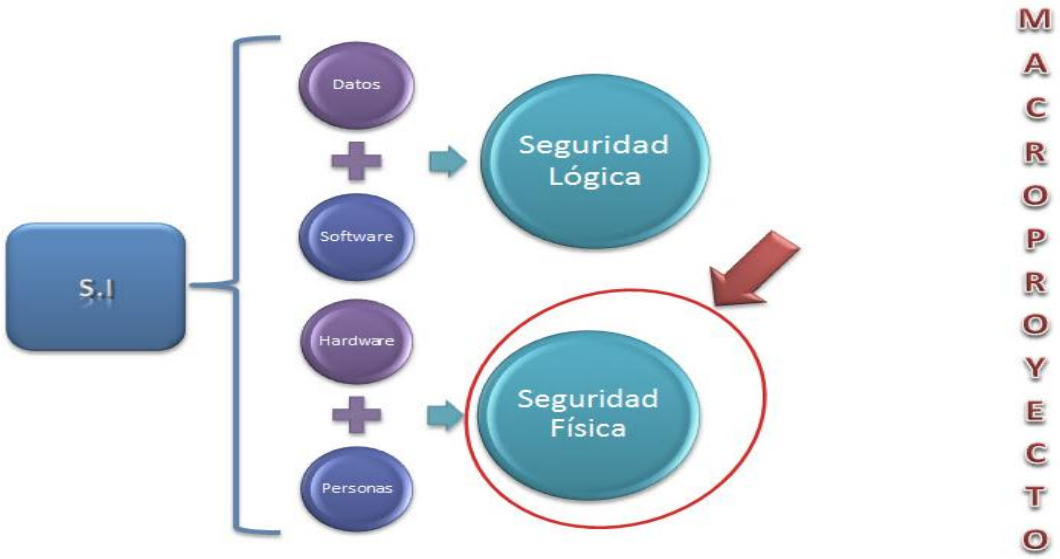


Figura 15. Elementos de la Seguridad Informática y forma de abordarlos. Fuente: Grupo de Trabajo.

A partir de la aplicación de las técnicas de recolección de información: Análisis de contenido, Observación no estructurada y Encuesta (Sondeo), y realizado el respectivo

análisis de resultados, el grupo de trabajo del presente proyecto determina como temática a desarrollar la Seguridad Física, dado que es uno de los aspectos más olvidados actualmente a la hora del diseño de un sistema informático, y uno de los más necesarios (Borghello C. , 2008). Si bien, se prevén algunos riesgos externos como virus, por ejemplo, otros como el acceso físico de un atacante interno a una sala de operaciones no se contempla. Lo que puede derivar que para un atacante sea más fácil tomar y copiar una cinta de la sala, que intentar acceder vía lógica a la misma.

En efecto, los requerimientos a nivel de seguridad son altos en la actualidad, debido a que los riesgos incrementan de forma vertiginosa. Las estadísticas muestran pérdidas financieras incalculables a raíz de incidentes que involucran ***fallas físicas***, y ***errores humanos***. La Open Security Foundation publica en la base de datos DatalossDB dentro de los incidentes de seguridad, en 2010, casos como: "*Ordenador portátil hurtado expone los nombres de 4.400 pacientes, el número de historia clínica, edad y datos clínicos", Empleado roba 100 solicitudes de hipotecas y comete fraude, El robo de una computadora de una oficina de matemáticas pone en riesgo calificaciones*". (Foundation, 2010). Cada uno de estos incidentes alcanza costos estimados de más de USD$3,000.00, por violación de datos. Además de consecuencias directas e indirectas para la organización y usuarios, que se convierten en traumáticas a la hora de reparar los daños causados.

Es claro, entonces, que las políticas de seguridad deben estar encaminadas de forma adecuada para proteger la información en todo sentido, prestando especial atención a los elementos que forman parte del procesamiento de información sensitiva o crítica del negocio, que deberán ser resguardados y protegidos por un perímetro de seguridad definido con controles apropiados de entrada. Este perímetro se marca a través de las Políticas de Seguridad Informática (PSI) a nivel de Seguridad Física, orientadas hacia tres aspectos principales: desastres naturales, amenazas ocasionadas por el hombre y sabotajes internos y externos deliberados. El objetivo es definir una serie de acciones a seguir en forma eficaz y oportuna para reducir los riesgos a los que se exponen los sistemas de cómputo e información, por ejemplo, incendios, fallas eléctricas, acciones hostiles, control de acceso físico, entre otros.

Teniendo en cuenta lo planteado, la investigación proyecta la disposición de una herramienta software, soportada en estudios de estándares internacionales, que oriente la labor de creación de *Políticas de Seguridad Física*. Y en consecuencia, comience a ser parte de la solución a los frecuentes problemas de seguridad informática en las organizaciones.

5.3. EVALUACIONES DE ESTÁNDARES INTERNACIONALES

En documentos oficiales de los estándares e informes, hallados en investigaciones y análisis de contenidos resumidos en los numerales 3.3 del Marco teórico y 5.1, se identificaron aspectos comunes que los caracterizan y permiten describir sus fines y forma de trabajar. Por lo tanto, éstos se listaron y posteriormente se adecuaron dentro de una matriz que permite evaluar los estándares equitativamente, en la medida en que se analiza como se comporta la norma en un mismo sentido tal como se muestra a continuación en la tabla 2; los elementos identificados son: objetivo, enfoque conformidad con sistemas de gestión, conceptos, modelo de proceso, cobertura y controles.

Estándar / Criterio	**Objetivo**	**Enfoque**	**Conformidad con sistemas de gestión**	**Conceptos (Incidente, Seguridad de la Inf.)**	**Modelo de Proceso**	**Cobertura**	**Controles (efectividad)**
ISO 27001	Proporcionar un modelo para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un SGSI.	Enfoque de proceso	Se alinea con ISO 9001:2000 e ISO 14001:2004	**Incidente:** un sólo o una serie de eventos de seguridad de la información no deseados o inesperados que tienen una significativa probabilidad de comprometer las operaciones comerciales y amenazan la seguridad de la información. **Seguridad de información:** preservación de la confidencialidad,	Modelo PDCA	Todos los tipos de organizaciones	Objetivos de Control y controles Anexo A. Tabla A.1 del documento 27001.pdf

				integridad y disponibilidad de la información; además, también pueden estar involucradas otras propiedades como la autenticidad, responsabilidad, no-repudio y confiabilidad.			
ISO 17799	Proporcionar un lineamiento general sobre los objetivos de gestión de seguridad de la información generalmente aceptados.	Enfoque sistemático	Al ser una recomendación solo indica los puntos a tener en cuenta cuando se implemente (virtualmente es compatible con todos los sistema de gestión)	**Incidente:** Un incidente de seguridad de la información es indicado por un solo evento o una serie de eventos inesperados de seguridad de la información que tienen una probabilidad significativa de comprometer las operaciones comerciales y amenazar la seguridad de la información. (ISO/IEC TR 18044:2004). **Seguridad de información:** preservación de la	Análisis del riesgo, evaluación del riesgo	Todos los tipos de organizaciones	

				confidencialidad, integridad y disponibilidad de la información; además, también pueden estar involucradas otras propiedades como la autenticidad, responsabilidad, no-repudiación y confiabilidad.			
COBIT	Brindar buenas prácticas a través de un marco de trabajo de dominios y procesos, y presenta las actividades en una estructura manejable y lógica. Vincular las metas de negocio con las metas de TI, brindando métricas y modelos de madurez para medir sus	Dominios y procesos. (Más Control, menos Ejecución)	• Comité de organizaciones patrocinadoras de la Comisión Treadway (**COSO**): *Control Interno—Marco de trabajo integrado*, 1994 • Oficina de comercio gubernamental (OGC®): Biblioteca de infraestructura de TI® (ITIL®), 1999-2004 • **ISO/IEC 17799:2005**, Código de prácticas para la administración de la seguridad de la información • Instituto de	Cobit no define específicamente los conceptos.	Modelo de procesos, el cual subdivide TI en 34 procesos de acuerdo a las áreas de responsabilidad de: *planear, construir, ejecutar y monitorear*.	Áreas de gobierno y control de TI de toda organización	Buenas prácticas y Objetivos de control

	logros, e identificando las responsabilidades asociadas de los propietarios de los procesos de negocio y de TI.		Ingeniería de Software (SEI®): SEI Modelo de madurez de la capacidad (CMM®), 1993 SEI Integración del modelo de madurez de la capacidad (CMMI®), 2000 • Instituto de administración de proyectos (PMI®): Cuerpo de conocimiento de administración de proyectos (PMBOK®), 2000 • Foro de seguridad de información (ISF): *El estándar de buenas prácticas para la seguridad de la información*, 2003				
ITSEC	Evaluación de las propiedades y características de seguridad de determinado producto o sistema IT (TOE)	**Criterios de Evaluación** para la evaluación de la corrección.	Diferentes criterios de seguridad TI en Europa(el francés, alemán),y una correspondencia parcial con las clases del TCSEC	ITSEC entre los conceptos que define no hace referencia estos	Define 7 de niveles de evaluación (E0, E1, E2, E3, E4, E5, E6) que representa el nivel de confianza	Organizaciones que incluyan hardware y software dentro de sus planes de gobierno	Evaluación de la eficacia, ataque directo (fuerza de los mecanismos. Tres niveles de resistencia se definen - básico, medio y alto) y La evaluación de la exactitud
TCSEC	Mantenimient	**Criterios de**	Se alinea con los	TCSEC no define	Define 7	Sistemas de	

	o de la confidencialidad de la información	**Evaluación** de la eficacia de Seguridad informática	Sistemas de Procesos de la organización, y estándares de recomendaciones aplicados	conceptos, sólo provee criterios para evaluar la eficacia de nuestros sistemas de Seguridad informática.	conjuntos de criterios de evaluación (D, C1, C2, B1, B2, B3, A1) denominados Clases.	Procesamiento Automático de Datos (ADP) disponibles en el mercado.	*Objetivos de Control*, Requisitos fundamentales de seguridad. *Clases*
Common Criteria	Definir un criterio estándar a usar como base para la evaluación de las propiedades y características de seguridad de determinado producto o sistema IT	Evaluación y certificación de la seguridad en Tecnologías de la Información, a través de *Requisitos funcionales y de garantía*		No presenta específicamente estos conceptos	Está divido en 3 partes que corresponden a: Modelo general, Requisitos Funcionales de Seguridad y Requisitos de Garantías de Seguridad	Organizaciones que manejen algún tipo de arquitectura informática y tecnológica	Proporciona unos niveles de garantía (EAL) como resultado final de la evaluación. EAL –Evaluated Assurance Level en un rango de 01 a 06.
RFC2196	Esta guía está dirigida a proporcionar una orientación básica en el desarrollo de un plan de seguridad para su sitio.	Enfoque generalmente aceptado a seguir es el propuesto por el autor Fites (Fites & Kratz, 1989). Que consiste básicamente	Al ser una guía solo indica los puntos a tener en cuenta cuando se implemente un esquema de seguridad para un sitio (virtualmente es compatible con todos los sistema de	No presenta específicamente estos conceptos en sus glosario	• Identificar qué objeto se está intentando proteger • Identificar de qué se está tratando de proteger al objeto	Está destinado principalmente a sitios que trabajan en el ambiente Internet. Pero también a	Evaluación de riesgos (Identificar los bienes e Identificar las amenazas)

		en 5 etapas.	gestión)		• Determinar cuáles son las probables amenazas • Implementar medidas que protegerán los bienes, medidas en costo/eficiencia • Revisar el proceso continuamente y efectuar las correcciones cada vez que se detecte un problema	aquellos sitios que permiten comunicarse con otros sitios. Y en forma general también puede ser utilizado en sistemas aislados.	

Tabla 2. Estudio de estándares por criterios de evaluación. a) ISO 27001. b) 17799. c) Cobit. d) ITSEC. e) TSEC. f) Common Criteria. g) RFC2196. Fuente: Grupo de Trabajo.

5.4. ANÁLISIS Y FUNDAMENTOS

Luego de evaluar los estándares por criterios establecidos, en este apartado se expone la técnica usada para compararlos, la cual está soportada en la teoría de la dualidad, expuesta a continuación en el primer ítem, con el propósito de establecer características orientadas hacia el diseño coherente del modelo de seguridad.

5.4.1. DUALIDAD DE LA SEGURIDAD INFORMÁTICA

Cada acción que realizamos siempre tiene una influencia en otras, y por consiguiente genera nuevos sucesos; lo que se denomina comúnmente como "efecto mariposa", donde un hecho da lugar a otro, ese a otros, y así sucesivamente. La base de esta dinámica del mundo es que *sin causas no habría efectos*, conocido en la literatura actual como Dualismo. Al llevarlo a la escala empresarial, por ejemplo, al finalizar el año se presentan los resultados de la gestión realizada, y los pronósticos del próximo año; de este modo, se relacionan los sucesos pasados con las posibles situaciones futuras.

La seguridad informática no es ajena a esta realidad, es quizá uno de los tópicos donde los especialistas en el área buscan afanosamente establecer líneas de acción sobre características especiales de los acontecimientos que pasaron y podrán ser influyentes en el futuro.

En este sentido, presentamos la estrategia de la dualidad, como una manera complementaria de explorar los hechos mismos en el mundo, para reconocer las causas y los efectos en su contexto, sin negar la posibilidad de considerar que uno surge a partir del otro, es decir, reconocer que la seguridad informática surge a partir de considerar la inseguridad informática y viceversa; un continuo de aprendizaje que muchas veces no corresponde a una causa específica sino a la relaciones existentes entre los componentes objeto del análisis. (Cano J. J., Inseguridad Informática: Un concepto dual en Seguridad Informática, 2010)

Por tanto, la inseguridad informática como disciplina dual en el estudio de la seguridad informática, permite comprender los posibles riesgos a los que están expuestos los sistemas

bajos situaciones extremas. En otras palabras, la forma cómo reaccionaría el sistema frente a ciertos incidentes, que pueden suceder teniendo en cuenta hechos pasados. Por lo tanto, mientras más se comprenda la realidad de la inseguridad, con mejores ojos podremos comprender la seguridad informática de las organizaciones.

En el desarrollo del presente proyecto, se tiene en cuenta el pensamiento dual aplicado a la seguridad informática, porque es una forma acertada de responder a las necesidades o requerimientos del mercado, además de que los fundamentos teóricos expuestos por los investigadores son coherentes con la dinámica mundial, lo que es fácilmente verificable. Así, siguiendo la línea metodológica propuesta para dar solución a la problemática, se indagan y analizan los incidentes de inseguridad informática a nivel de seguridad física en las organizaciones, que reflejan la realidad actual sobre la cual se basará el diseño del Esquema de Seguridad.

A continuación, se presenta el estudio realizado a la base de datos facilitada por la OSF (Open Security Foundation)[9], que reporta hechos de inseguridad a nivel mundial. Así mismo, en la sección siguiente, algunos apartes de la II encuesta latinoamericana de seguridad informática, que evidencia el estado y tendencias de Colombia y otros países. Los mismos constituyen el fundamento para la evaluación de los estándares internacionales y posterior comparación y selección de elementos que harán parte del modelo (más adelante en la sección 5.4.4).

[9] Para ampliar información, consultar la fuente: (Foundation, 2010).

5.4.2. BASE DE DATOS DATALOSS DB - REPORTE MUNDIAL

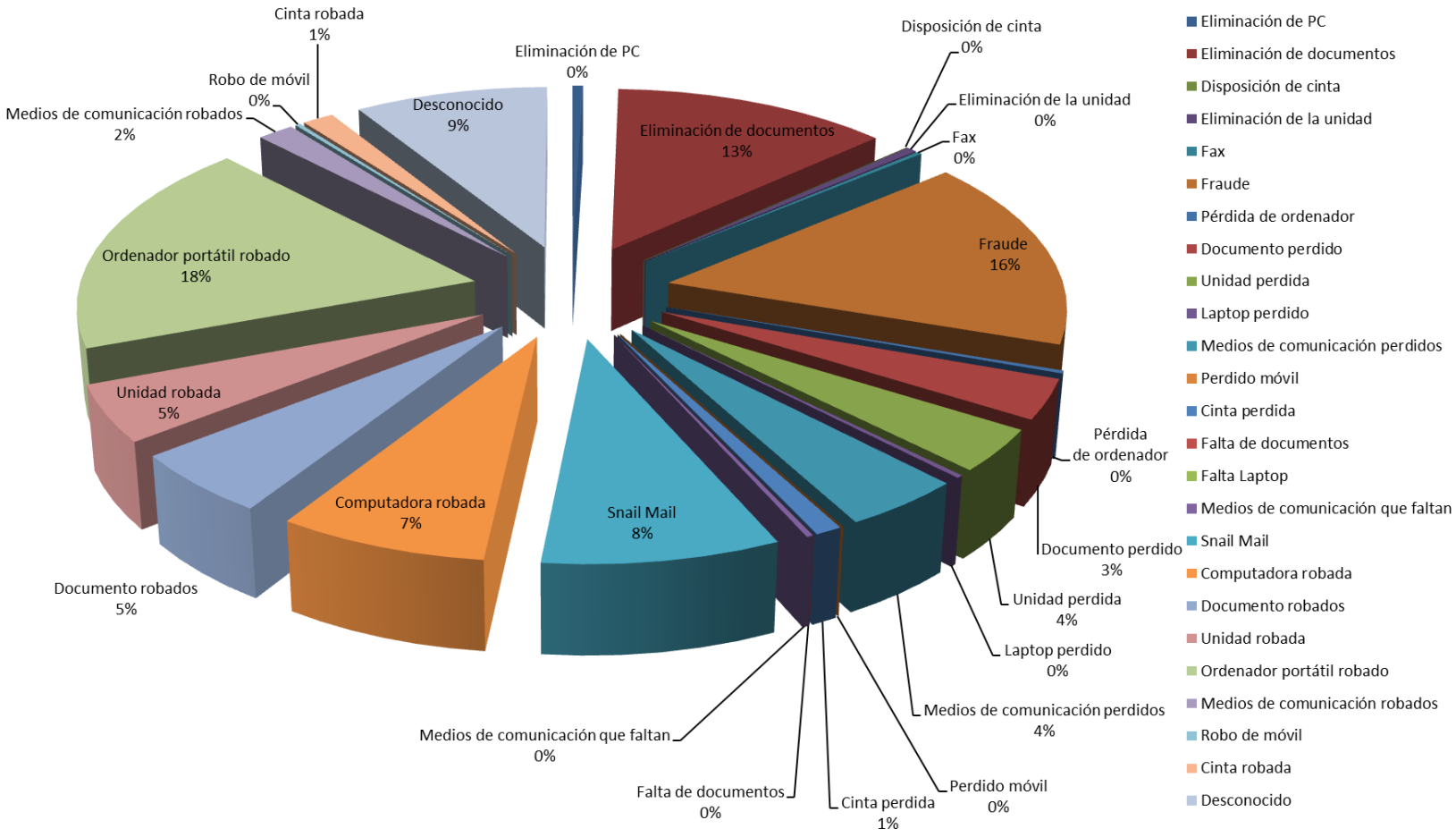


Figura 16. Incidentes reportados de acuerdo a su clasificación por tipo. Fuente: Grupo de Trabajo, con base en (Foundation, 2010).

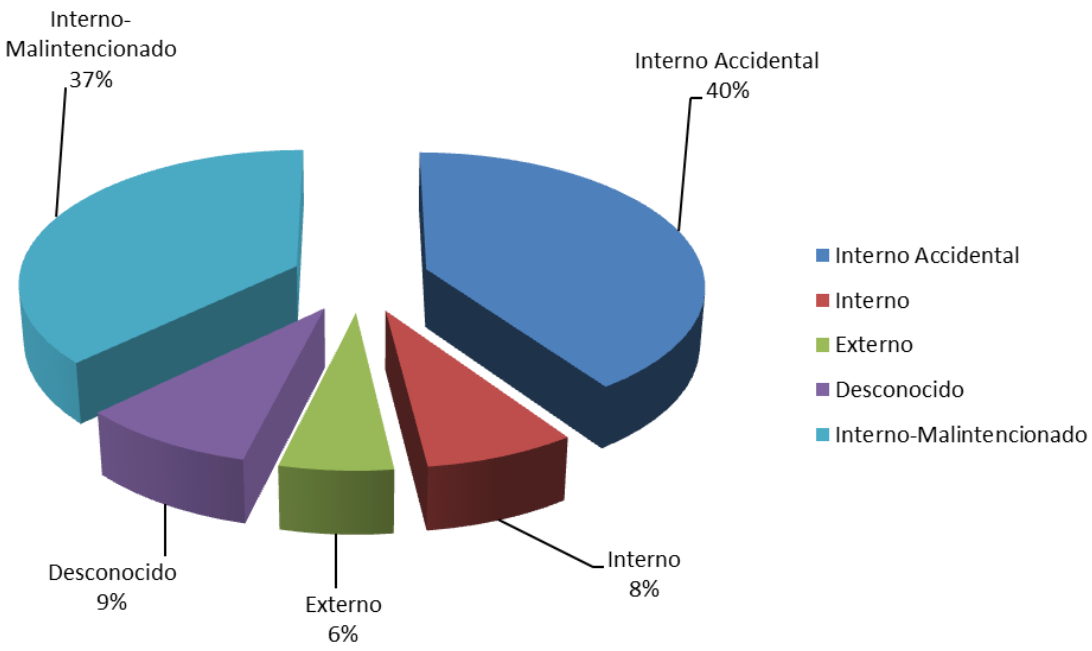


Figura 17. Incidentes de acuerdo a origen o procedencia en la organización. Fuente: Grupo de Trabajo, con base en (Foundation, 2010).

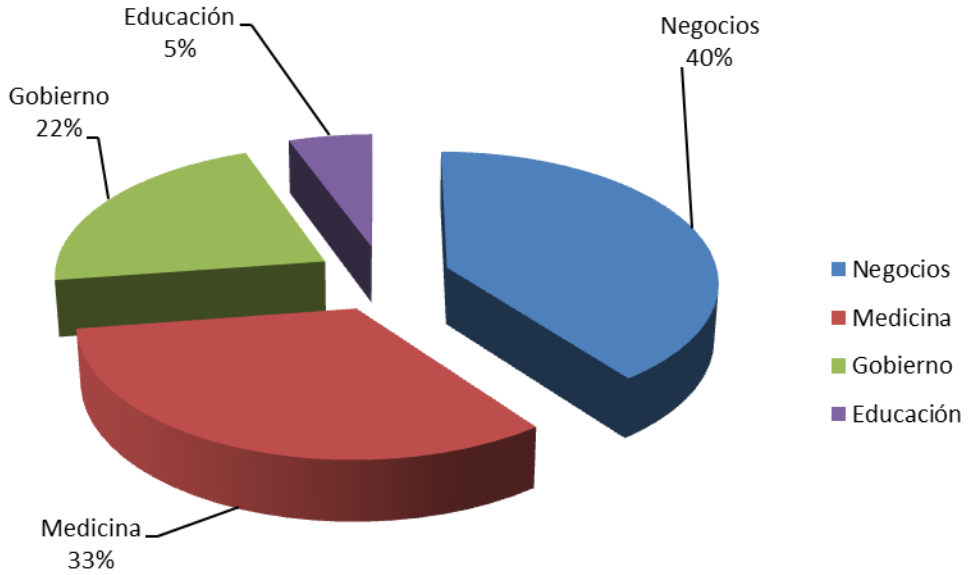


Figura 18. Distribución de Incidentes reportados por tipo de negocio afectado. Fuente: Grupo de Trabajo, con base en (Foundation, 2010).

ANÁLISIS DE GRÁFICOS

Para **2010** según los Tipos de incidentes:

- ***Ordenador portátil robado*** fue el incidente con mayor porcentaje de ocurrencia con un 18%, es decir, el caso más frecuente en las empresas para este año fue el robo de los portátiles a raíz de fallas en el acceso físico a las instalaciones.
- Seguido del ***Fraude*** con un 16% y la ***Eliminación de documentos*** con una participación del 13% sobre el total.
- De la misma forma, el estudio muestra que los problemas más comunes en las organizaciones después de los mencionados, estuvieron relacionados con el robo y pérdida de cintas, documentos y unidades (figura 16).

De acuerdo a las estadísticas reflejadas en la figura 17,

- Los incidentes que han afectado a las empresas para este periodo de tiempo tiene su origen al ***Interior*** de las mismas, lo que significa que las pérdida de dato traducida en pérdidas financieras, a partir de ordenadores portátiles robados, fraude, eliminación de documentos como principales, provienen de actuaciones internas, ocasionadas su mayoría por accidentes, pero también por hechos malintencionados (40% y 37% respectivamente),
- Además han sido organizaciones comerciales o de Negocios las más afectadas según los reportes presentados, seguidas de entidades de medicina, gobierno y finalmente, educación con una incidencia bastante mínima (figura 18).

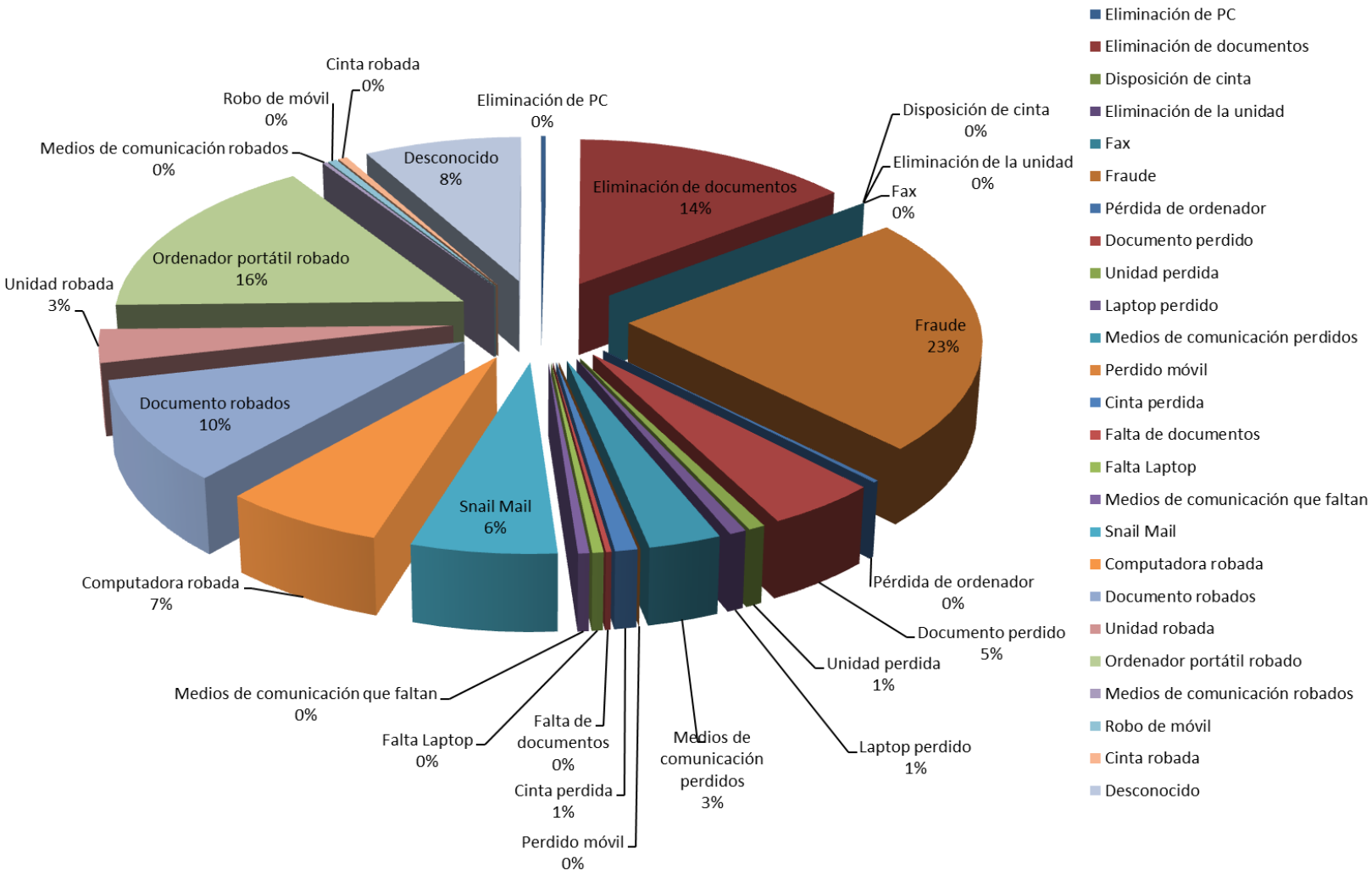


Figura 19. Incidentes reportados de acuerdo a su clasificación por tipo. Fuente: Grupo de Trabajo con base en (Foundation, 2010).

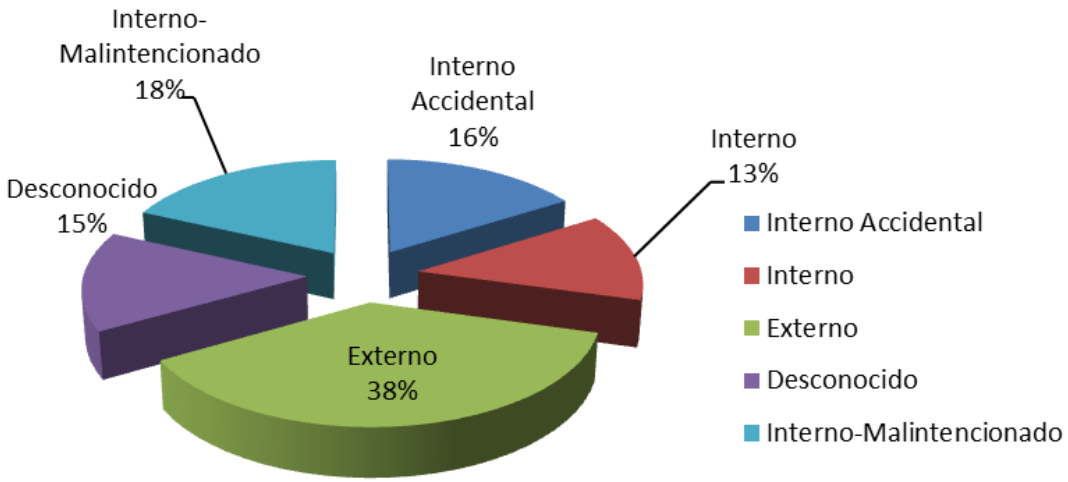


Figura 20. Incidentes de acuerdo a origen o procedencia en la organización. Fuente: Grupo de Trabajo con base en (Foundation, 2010).

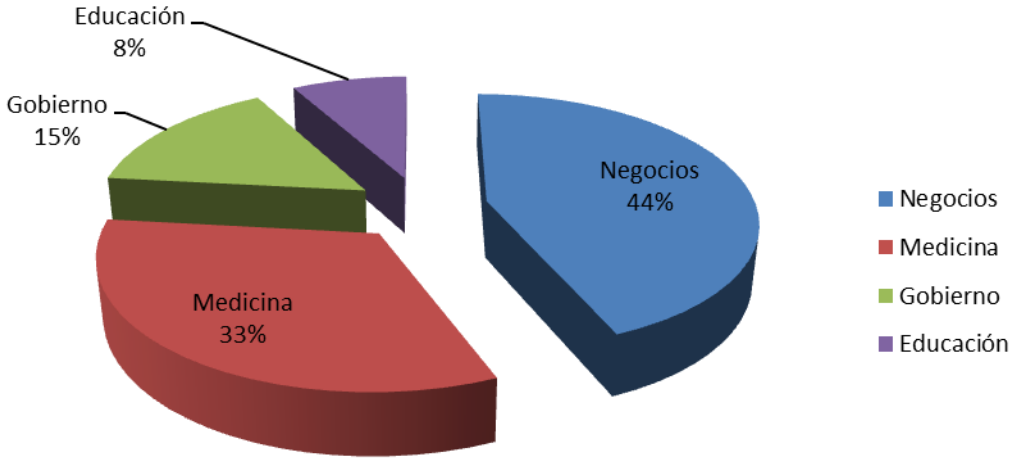


Figura 21. Distribución de Incidentes reportados por tipo de negocio afectado. Fuente: Grupo de Trabajo con base en (Foundation, 2010).

Para el año **2011** las estadísticas varían en algunos aspectos:

- El ***Fraude*** ocupa el primer lugar como el incidente más reportado en las empresas para este año, seguido, coherentemente con el año anterior, por el robo de portátiles,

y la eliminación de documentos, igualmente, el robo y pérdida de elementos como cintas, unidades, y documentos son hechos que se siguen presentando (figura 19). Así mismo, como se ilustra en las figuras 20 y 21

- El origen de incidentes en el 38% de los casos es ***Externo***, siendo ésta la mayor incidencia, seguido de los provocados al interior de la empresa, ya sea accidentales o malintencionados, con el 16% y 18% respectivamente. Del 15% del total de los hechos reportados se desconoce su origen, lo que es un porcentaje bastante representativo de casos que no se han determinado.
- Empresas comerciales o de ***Negocios*** siguen siendo las más afectadas, con un alto porcentaje, siguiendo la línea las de Medicina, Gobierno y Educación, al igual que en 2010.

5.4.3. ESTADÍSTICAS Y TENDENCIAS EN COLOMBIA Y PAISES DE LATINOAMÉRICA

La II Encuesta Latinoamericana de Seguridad de la Información, ACIS 2010, contó con la participación de empresas de Argentina, Chile, Colombia, México, Uruguay, Paraguay y otros (Venezuela, Perú, Costa Rica, España, Bolivia). Los resultados estadísticos más relevantes para el proyecto, son ilustrados en los gráficos siguientes.

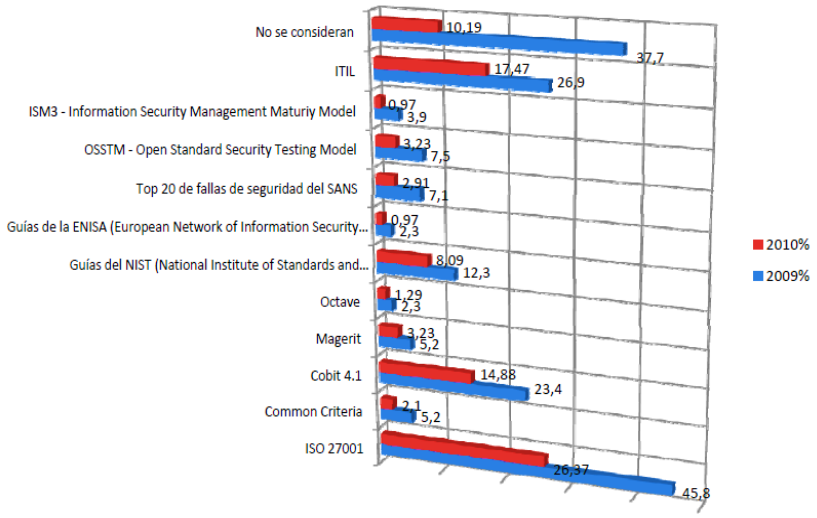


Figura 22. Estándares y buenas prácticas de seguridad. Fuente: (Cano & D, 2010).

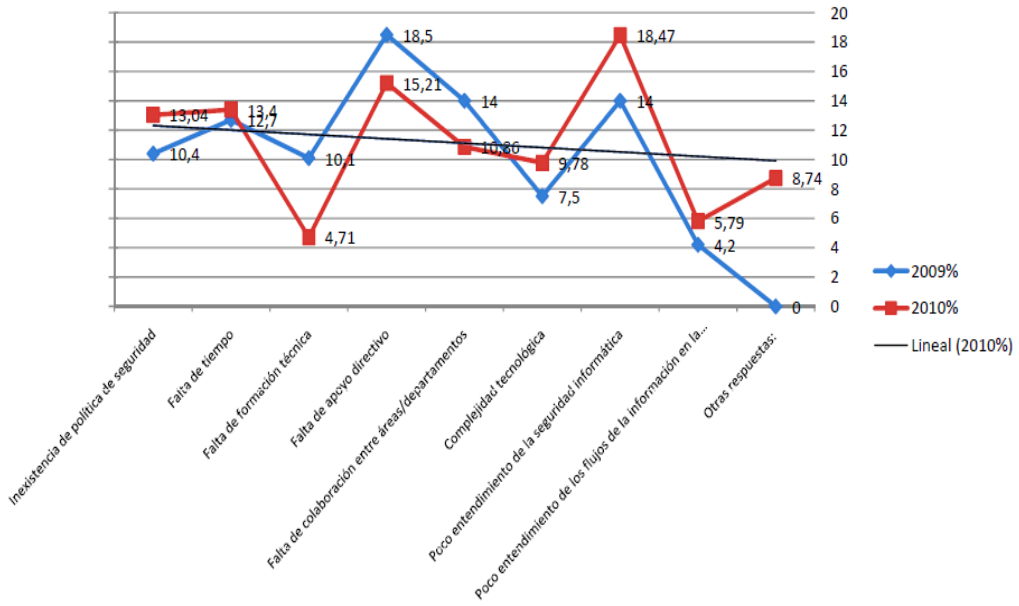


Figura 23. Obstáculos para implantar seguridad informática. Fuente: (Cano & D, 2010).

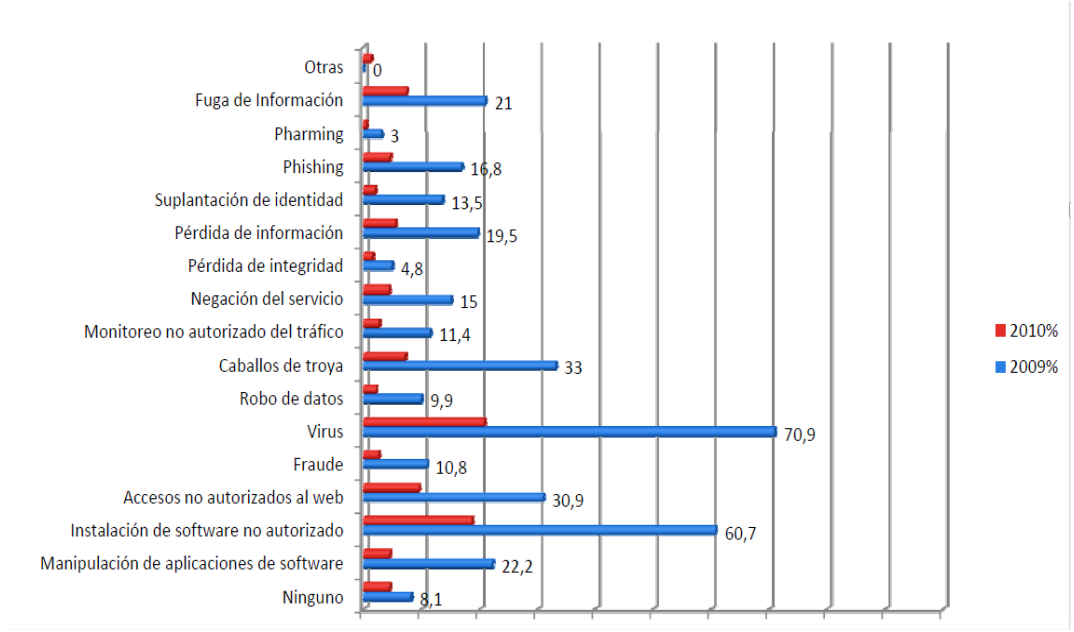


Figura 24. Fallas o incidentes de seguridad informática. Fuente: (Cano & D, 2010).

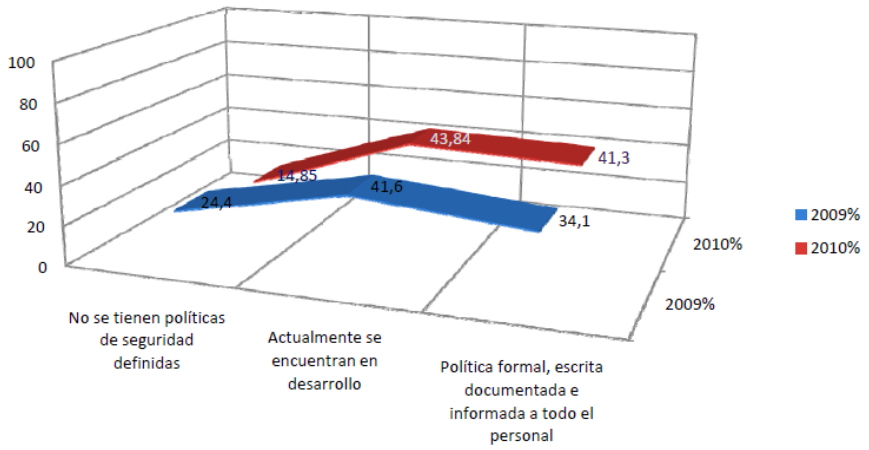


Figura 25. Estado de las empresas en relación a políticas de seguridad informática. Fuente: (Cano & D, 2010).

Siendo nacionales el 58,90% de los encuestados, la encuesta revela que ISO 27001 es el estándar más aplicado, seguido de ITIL y COBIT. El ***poco entendimiento*** de seguridad informática (18,47%) es el principal obstáculo para implantar SI en las empresas para 2010, con incremento de 4,47% en relación al año anterior, y en segundo lugar la ***falta de apoyo directivo*** con un 15,21%. Aunque de 2009 a 2010 hay más apoyo directivo, son más lo que manifiestan desconocer o entender el tema de seguridad informática.

La ***falta de tiempo*** es un factor importante que impide implantar seguridad informática de la mano de inexistencia de políticas. Se destaca mayor formación técnica.

Se evidencia un aumento en ***complejidad tecnológica***, que puede ser influyente directo en el poco entendimiento de los temas de seguridad, como obstáculo principal en la implantación. Se muestra que los ***virus, los troyanos y la instalación de software no autorizado*** son la principal forma de ataques presentados. Cabe destacar que, aunque se conservan las proporciones de ocurrencia de incidentes, la reducción de 2009 a 2010 es evidente. Finalmente, se muestra un leve incremento de políticas en desarrollo, y un importante crecimiento en políticas formalmente definidas.

5.4.4. COMPARACION DE ESTÁNDARES POR CRITERIOS ESTABLECIDOS

En la etapa de comparación de los estándares para la selección de características y elementos que permitieran construir el esquema de solución propuesto en la investigación, el primer asunto a resolver fue determinar, precisamente, con qué criterios compararlos para elegir una u otra característica cumpliendo con los requisitos. En respuesta, se plantearon diferentes opciones a lo largo del proceso, que es pertinente mostrar; inicialmente, se propuso la identificación de estas características con base en *cómo los estándares respondían y/o aplicaban cada una de las etapas del Ciclo de vida de una política de seguridad informática, y a partir de allí construir los cuadros y seleccionar características de cada uno,* sin embargo, al analizarla, se encontró que no era el método adecuado debido a que los estándares no especifican el proceso de creación de políticas, dicen qué se debe hacer, incluyen sus propios enfoques, métodos y procesos para contribuir a la seguridad. Además, no están hechos específicamente hacia PSI, si no, a la seguridad de la organización mediante un SGSI (que incluye políticas) seguro u otros medios. Por lo anterior, se descartó esta metodología.

En segunda instancia, se formuló *analizar cómo los estándares respondían o abordaban las necesidades en las organizaciones actualmente, identificando éstas a través de una encuesta a nivel nacional sobre la aplicación de los estándares seleccionados en la investigación;* de esta forma, dividiendo la encuesta en grupos de preguntas por criterio, por ejemplo, preguntas sobre el objetivo, otras del enfoque, del modelo de proceso, y así sucesivamente, donde serían los encuestados quiénes determinarían el nivel de respuesta de los estándares a sus requerimientos, evaluándolos por partes. Realizado esto, el resultado final daría los puntajes recibidos por elemento de cada estándar, lo que permitía la selección de los más altos, dando lugar al modelo o esquema de seguridad. La técnica descrita, aparentemente, es consistente y su fundamentación es sólida, porque se basa en un estudio de opiniones del mercado, que en últimas es lo que interesa a los investigadores; que el proyecto tenga acogida en la medida en que cubre necesidades reales. No obstante, al iniciar su desarrollo, se determina que las empresas nacionales no son un buen referente dado que en Colombia la aplicación de normas y estándares es escaza, de acuerdo a

estudios (Cano & D, 2010); además, en el caso de conocer sobre los estándares sería complejo para las empresas responder en tanto detalle, pues sus conocimientos son limitados, lo que implica que los resultados de las encuestas no serían confiables, y el modelo final estaría alejado de los requisitos reales.

En este sentido, de la idea anterior se rescata que, indiscutiblemente, ***el Modelo debe construirse con base en las necesidades actuales del mercado***, no sólo a nivel nacional sino mundial. Consecuentemente, se replantea la metodología: se proyecta un estudio de la realidad del mercado, enfocado más bien a lo que se está presentando en cuanto a inseguridad informática en las empresas, teniendo en cuenta la teoría de la dualidad explicada anteriormente (sección 5.4.1), es decir, en lugar de preguntar a las empresas cómo responden los estándares a sus requerimientos, se va a evaluar cuáles son los requerimientos de las empresas a nivel de seguridad física, y a partir de allí el grupo de trabajo determinará si los estándares responden a éstos, cómo y mediante qué elementos lo hacen, con la finalidad de extraer características acordes a lo sucedido actualmente y lo que posiblemente ocurrirá con base en eso, fundamentado en la seguridad informática como un concepto Dual.

En este orden de ideas, el estudio de la inseguridad en las organizaciones, que se traduce en las fallas e incidentes presentados, se realizó gracias a un trabajo desarrollado por la Open Security Foundation a través de la base de datos DataLossDB que almacena reportes anuales clasificados por meses, tipos de incidentes, fuente, entre otros. Lo que el grupo de trabajo realizó fue una depuración de la base de datos DataLossDB, seguidamente, la representación gráfica de los reportes, y su respectivo análisis (expuesto en la sección 5.4.2). Así como una breve recopilación de encuestas y tendencias en Colombia y otros países latinoamericanos.

En síntesis, a partir de las evaluaciones realizadas a los estándares internacionales, en esta etapa, se comparan los mismos con la finalidad de extraer de cada uno los elementos que cumplen con los requerimientos del mercado o abarcan de alguna forma incidentes de seguridad física evidenciados en los estudios estadísticos mencionados.

La comparación de estándares se realiza haciendo un paralelo entre los aspectos de cada uno plasmados en las columnas de la tabla 3 (Objetivo, enfoque, conformidad con sistemas de gestión, conceptos, modelo de proceso, cobertura y controles). De acuerdo al siguiente criterio: Se estipula un rango de 1 a 5, donde 1 significa que ese aspecto del estándar *no aplica* a las necesidades del mercado, estadísticas y teorías actuales, según el concepto del evaluador; y 5 que el elemento del estándar *aplica totalmente*, abarca los requerimientos y cubre la concepción del evaluador según los estudios y análisis realizados.

Estándar / Criterio	**Objetivo**	**Enfoque**	**Conformidad con Sistemas de gestión**	**Conceptos**	**Modelo de Proceso**	**Cobertura**	**Controles (efectividad)**
ISO 27001	2	4	5	4	5	5	4
ISO 17799	1	3	5	5	3	5	1
COBIT	5	5	4	2	3	4	4
ITSEC	1	2	1	1	2	2	3
TCSEC	2	3	5	1	3	4	5
Common Criteria	3	3	2	1	2	5	5
RFC2196	4	1	2	1	5	2	4

Tabla 3. Valoración de estándares de acuerdo a análisis, fundamentos, y concepto de investigadores.

El resultado de la evaluación, realizada por investigadores del grupo de trabajo es el siguiente:

- Objetivo: COBIT – RFC
- Enfoque: COBIT (Dominios y Procesos- Alineación estratégica)
- Conformidad: ISO 27001
- Conceptos: ISO 17799
- Modelo de proceso: RFC – ISO 27001
- Cobertura: ISO 27001 – ISO 17799
- Controles: TCSEC

El **objetivo** de COBIT está orientado a ofrecer buenas prácticas basadas en *vincular las metas del Negocio con las metas de Tecnologías de Información*, ofreciendo métricas y modelos de madurez para medir sus logros; identificando las responsabilidades de los funcionarios en ambas partes. Por lo tanto, al tener presente los objetivos de la empresa para establecer medidas de seguridad, se garantiza que la estrategia de SI fluya de forma gradual en la organización así como los planes del negocio; de este modo, no se dejan brechas de seguridad física en áreas de la misma que facilitan el acceso a la información a través de la sustracción de equipos de cómputo portátiles, cintas, por ejemplo. Además, se vincula todo el personal en las actividades programadas, al acoplar las políticas a sus tareas correspondientes; desde los operarios, hasta los miembros de gerencia quiénes tienen la responsabilidad de brindar el apoyo directivo necesario, además de ser parte del cumplimiento de las medidas implantadas. Adicionalmente, RFC 2196 plantea *proporcionar una orientación básica en el desarrollo de planes de seguridad*, un objetivo básico pero coherente con el proyecto.

El **enfoque** de COBIT, es el relacionado en su objetivo, por lo que es coherente a los requerimientos del mercado, se resume en: procesos y alineación estratégica.

En relación a la **conformidad con los sistemas de gestión**, se considera ISO 27001 como un buen modelo a seguir, porque es un estándar aceptado internacionalmente, que se alinea a normas, estándares más conocidos y sistemas internos en las empresas. La alineación se da en la medida en que es adaptable a sistemas implementados en la empresa, además, no contiene ninguna cláusula que impida ser trabajado en conjunto con otras normas o modelos.

La definición de **conceptos** ofrecida por ISO 17799 es amplia, y conforme no sólo a lo conceptualizado a nivel nacional, sino también lo reportado en la base de datos mundial y estudios analizados.

El **Modelo de Proceso**, es de suma importancia en esta evaluación, pues define la línea de actuación a seguir en el Modelo de Seguridad que se diseñará; esto es, le da la forma o estructura a alto nivel, que responderá a los requerimientos. Por lo tanto, debe ser sencillo y fácil de entender, con la finalidad de que reduzca la falta de entendimiento y complejidad de aplicación de seguridad informática, expuesta en el planteamiento del problema y evidenciada en la encuesta (sección 5.4.3). En este sentido, RFC 2196 e ISO 27001 reúnen una serie de características que es conveniente rescatar:

RFC 2196 plantea un conjunto de pasos que resguardan de forma básica y eficiente la disponibilidad, confiabilidad e integridad. Tiene presente determinar: qué se debe proteger, de qué y cómo hacerlo, analizando las probables amenazas del medio, y finalmente, realiza una revisión continua de resultados para la aplicación de correcciones precisas de acuerdo a éstas.

Al hacer un paralelo entre esta idea y los requisitos reflejados en análisis anteriores, existe correspondencia, así: los principales problemas están relacionados con fallas de acceso físico, que conllevan a pérdida y hurto de recursos que contienen información crítica de la empresa. Por otra parte, es clara la alta incidencia interna, accidental o malintencionada; además, el fraude mediante técnicas de Ingeniería Social en el último año afectó representativamente las empresas a nivel mundial; lo que quiere decir que el recurso humano (interno y externo) es un elemento clave en estos hechos. Así mismo, se puede inferir falta de control y medidas para garantizar resguardo, manejo y aprovechamiento

adecuado de la infraestructura tecnológica (altos porcentajes de virus, instalación de software no autorizado y aumento de complejidad tecnológica manifestada son muestras de ello). En respuesta, el estándar propone realizar una evaluación de riesgos a través de la determinación de los bienes a proteger en la empresa y las amenazas que pueden existir en su contra, lo que involucra la toma de decisiones costo/beneficio. En otras palabras, al identificar qué es lo realmente prioritario para la organización y los riesgos latentes, dentro de los cuales pueden estar implicadas fallas del personal interno e inseguridad en el contexto, reflejada en estudios y reportes,[10] se crea un perímetro de seguridad sólido orientado a la necesidad real, que indica hacia dónde enfocar los esfuerzos, sin malgastar recursos. Consecuentemente, constituye un método viable para involucrar al personal en los procesos de seguridad informática instruyéndolo sobre las técnicas de ingeniería social, que deben afrontar.

La revisión frecuente y manejo de correcciones facilita acatar la detección de nuevas amenazas e identificación de nuevos objetos a proteger prioritariamente, lo que sugiere un ciclo de trabajo que no admite vacíos de seguridad, principalmente a nivel físico (que es el interés investigativo). En tal dirección, como afirma Jeimy J. Cano, es necesario reconocer que sólo mirando las posibilidades de falla y vulnerabilidad, es posible mejorar la práctica misma de la administración de riesgos y la definición de mecanismos de seguridad y control (Cano J. J., Aprendiendo de la Inseguridad Informática, 2010).

En relación a lo anterior, se destaca que el orden de trabajo PDCA (Plan Do Check Act) brindado por el estándar ISO 27001 guarda estrecha correlación con las etapas establecidas (RFC 2196), caracterizándose por su baja complejidad de aplicación; por lo tanto, la línea adoptada, se haría más factible al realizar un enlace conceptual entre estas metodologías (véase sección 5.6 de estructura del modelo).

El propósito del esquema es brindar **cobertura** a todas las organizaciones, como lo señala ISO 27001 y otros estándares.

[10] Por lo tanto, este proceso responde a los requerimientos del mercado, al tener en cuenta los hechos de inseguridad. Formalmente es aplicar *dualidad de la seguridad informática.*

Respecto a los **controles** se considera que TCSEC propone buenas pautas para evaluar un determinado sistema de gestión de seguridad, pues engloba políticas, responsabilidad y garantía como criterios principales, estipulando requisitos a cumplir para cada uno, por ejemplo: identificación, seguridad, protección continua, entre otros. El objetivo es tomar estos criterios para controlar el cumplimiento de todos los aspectos de seguridad necesarios en la empresa.

5.5. ESTUDIO DE ESTÁNDARES Y GUÍAS DE SEGURIDAD FÍSICA EN CENTROS DE CÓMPUTO

Al concebir la seguridad física como un marco que permite la aplicación de barreras físicas para proteger la información, infraestructura y operaciones de la organización, de riesgos a amenazas que atentan contra su integridad, atendiendo, principalmente, daños por accesos físicos no autorizados e ingeniería social, este apartado hace una breve relación de aspectos generales a tener en cuenta en cualquier tipo de organización al momento de implantar políticas de seguridad física; éstos se ajustarán dependiendo la necesidad de la empresa. En el software de materialización del modelo EBASF, son engrosados como parte de las sugerencias ofrecidas en la etapa de creación de medidas (etapa 2 del modelo, sección 5.6). Orientando al encargado en la determinación del ámbito de seguridad que debe atender.

Aspectos genéricos de Seguridad Física, en Centros de Cómputos:

- Perímetros de seguridad física
- Controles de acceso físico
- Protección de oficinas e instalaciones
- Desarrollo de tareas en áreas protegidas
- Aislamiento de las áreas de recepción y distribución
- Ubicación y protección del equipamiento y copias de seguridad
- Suministros de energía
- Seguridad del cableado
- Mantenimiento de equipos

- Seguridad de equipo fuera de instalaciones
- Destrucción y re-uso seguro de equipos
- Políticas de escritorios y pantallas limpias
- Retiro de los bienes
- Elementos de trabajo
- Controles en servicios prestados
- Manejo de ataques potenciales de ingeniería social
- Principios fundamentales hacia el personal interno

5.6. ESTRUCTURACIÓN DEL ESQUEMA DE REFERENCIA DE SEGURIDAD INFORMÁTICA

La dinámica actual de las organizaciones exige de éstas un aprendizaje permanente para mantener los altos niveles actuales de operación y aumentar la capacidad de reacción ante las eventualidades en el desarrollo de sus negocios (Cano J. J., Aprendiendo de la Inseguridad Informática, 2010). Paralelamente, la inseguridad informática evoluciona y propone nuevos retos a las empresas que se manifiestan en variables humanas, técnicas o procedimentales, impactando los activos más importantes para las organizaciones.

De esta forma, se hace necesario que las empresas implementen medidas de seguridad que le permitan establecer una línea estratégica de continuidad en el futuro.

El esquema de referencia de seguridad informática diseñado como resultado de las investigaciones, es una forma de lograr este objetivo; porque es un modelo básico de seguridad que reúne características y elementos estratégicamente adaptados e integrados, fundamentados en la problemática preestablecida y los requerimientos actuales, desde una perspectiva dual de seguridad.

Más adelante, la figura 27 muestra el esquema propuesto, denominado **EBASF** (Esquema Básico de Seguridad Física) estructurado de la siguiente forma:

Objetivo: Brindar buenas prácticas, a través de una orientación básica en el desarrollo de políticas de seguridad, vinculando las metas del negocio, con las metas de Tecnologías de Información de la organización.

Enfoque: Modelo orientado a procesos. Aplicación de alineación estratégica en la creación de políticas de seguridad física.

Modelo de Proceso: Cuatro (4) etapas comprenden el modelo de proceso, las cuales están organizadas de acuerdo al orden de trabajo del PDCA; al cumplirse la última, se pueden reiniciar las actividades, convirtiéndose en un el ciclo de trabajo.

Sin embargo antes de abordar el recorrido por las etapas, el modelo de proceso incluye el diligenciamiento de un formulario[11] que consta de una serie de preguntas que indagan la naturaleza de la organización, con la finalidad de construir un referente del campo de acción a tratar. No es posible continuar la aplicación del modelo EBASF sin culminar este paso. Al concluirlo, se continúa con el proceso:

1. Planear**:** *Identificar el objeto a proteger, identificar de qué se intenta proteger.*

Concretado el Sondeo Inicial a la empresa, el encargado debe listar los bienes a proteger de acuerdo a categorías sugeridas (tabla 4). Así mismo, los problemas presentes o fallas físicas de qué protegerlos, organizándolos por nivel de gravedad.

Hardware	**Datos**	**Personal**	**Servicios**	**Redes**	**Soporte de información**	**Equipamiento auxiliar**	**Instalaciones**
Nivel de Gravedad	**Descripción del problema**						
1							
2							
3							

Tabla 4. Categorías para clasificar los bienes. Problemas. Fuente: Grupo de Trabajo.

[11] Se presenta el formulario de sondeo en la herramienta software que implementa el modelo EBASF. Éste formato es diligenciado una sola vez por el usuario del sistema.

La lista puede modificarse o expandirse en la medida que sea necesario reiniciar el ciclo al cumplirse la última del proceso. Es decir, si la revisión general aporta resultados que asocian problemas y/o activos no identificados o tratados en la primera ejecución de modelo de trabajo EBASF.

2. Hacer**:** *Implementar medidas de seguridad, teniendo en cuenta la relación costo/eficiencia.*

Realizado el plan de objetos y problemas a tratar, el siguiente paso consiste en determinar políticas orientadas a rectificar la situación. Para ello, debe seguirse un proceso denominado Ciclo de Vida de PSI (figura 26), que consiste en cuatro fases, cada una de las cuales comprende etapas a cumplir, que van desde la creación de la política hasta su eliminación.

En el desarrollo, que es la fase principal del procedimiento, se debe prestar especial atención a la orientación, alcance, y objetivos de la política que se diseña, porque de esto depende la eficacia del esquema; por lo tanto, se toma como referente aspectos de seguridad física planteados anteriormente, en la sección 5.5. Igualmente, el modelo ofrece sugerencias, que están fundamentadas en el análisis del sondeo diligenciado; éstas son pautas que orientan al encargado hacia gestión de necesidades propias de la organización, ubicándolo en una línea de actuación adecuada.

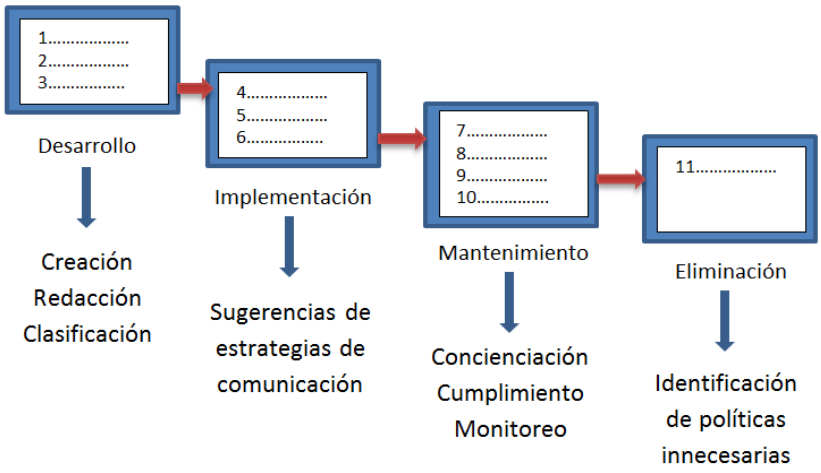


Figura 26. Proceso a realizar en la etapa Hacer, del modelo. Fuente: Grupo de Trabajo.

Además de lo anterior, es imprescindible revisar la lista de metas de negocio de la compañía antes de redactar y proponer las medidas de seguridad física, se debe asegurar que no vayan en contra de las actividades productivas y administrativas, contrario a esto, cada política debe mantener una correspondencia con las principales metas de negocio. En otras palabras, si una de las misiones de una entidad educativa es brindar educación de calidad, por ejemplo, y se les impide a los estudiantes el uso de los equipos de cómputo para realizar investigaciones, fuera de los horarios de clases, por cuestiones de seguridad física; a pesar de estar garantizando de algún modo la integridad de las máquinas, se está entorpeciendo el proceso de aprendizaje. De este modo, no existe alineación entre las metas de seguridad informática y las organizativas. El presente modelo adopta una matriz que permite evidenciar y registrar la correspondencia de cada una de nuestras políticas con los propósitos de negocio preestablecidos, relacionando estratégicamente las metas de ambas partes con *los requisitos fundamentales de seguridad*, que corresponden a los controles del modelo (figura 23), y los Objetivos de Seguridad Informática (véase más adelante).

Es pertinente aclarar algunos aspectos importantes en esta segunda etapa del modelo:

- Cuando se realiza por primera vez el proceso, en esta etapa (Hacer) sólo se llega a la primera fase del ciclo de vida de las políticas, porque hasta ese momento, éstas no pueden ser implementadas aún, dado que son políticas iniciales que requieren ser completadas, por consiguiente, no requieren mantenimiento o eliminación; sólo son creadas, revisadas y aprobadas.
- La continuación del proceso, específicamente la etapa 3, permite identificar amenazas que eventualmente no habían sido contempladas al diseñar las primeras políticas, por lo que, es conveniente reiniciar el proceso, haciendo el listado formal de los activos que se verían afectados por los probables ataques determinados y adicionar políticas adecuadas que complementan la estrategia de seguridad.
- La adición de políticas de seguridad en repeticiones del ciclo de trabajo, se darán de acuerdo a la relación costo/eficiencia, es decir, midiendo qué tan conveniente es para la empresa asumir la amenaza o atenderla, contrastando el valor de lo que se perdería con el costo de implantar la medida.

3. Monitorear**:** *Determinar probables amenazas y revisar políticas*

Una vez se han creado las políticas preliminares que cubren los problemas visiblemente identificados en la empresa, se determinan probables amenazas que, igualmente, pueden causar daños a los bienes listados. En otras palabras, aunque son riesgos latentes, no visibles para la organización llegarían a afectarla, debido a la alta probabilidad de que sucesos pasados generen incidentes en el presente que podrían afectar proyecciones futuras, fenómeno científicamente conocido como dualismo (mencionado anteriormente). Esta evaluación se lleva a cabo mediante un Análisis de Riesgos a través de la metodología MAGERIT 2.0[12]. Luego se registran las amenazas encontradas. De acuerdo a los resultados, se deben revisar las políticas creadas con la finalidad de conocer el nivel de cubrimiento que brindan a las posibles amenazas.

4. Actuar**:** *Revisar el proceso y aplicar correcciones o mejoras necesarias*

En esta etapa, corresponde hacer una revisión general del proceso, desde las políticas creadas, las estrategias de comunicación y cumplimiento de las mismas, hasta la alineación estratégica aplicada, el cumplimiento de los requisitos fundamentales de seguridad informática preestablecidos, entre otros aspectos. Todo esto con el propósito de aplicar correcciones o mejoras necesarias, y si es necesario, dar paso hacia la etapa 1, de *identificación de objetos a proteger*, para registrar problemas, que no habían sido tenidos en cuenta, o por lo menos no estaban en una posición prioritaria en la escala de gravedad, y que deben estarlo de acuerdo a los riesgos e impactos hallados en el análisis de riesgos de la etapa anterior (monitorear).

Política		**Nivel de cumplimiento (1-5)**	**Alineación estratégica (SI-NO)**	**Problema(s) identificado(s)**	**Observación (es)**
1					
2					

[12] Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Ministerio de administraciones públicas. Madrid. (Crespo, 2005).

3 ...					

Tabla 5. Revisión general del proceso. Fuente: Grupo de Trabajo.

Activo	Amenaza	D	RR-IR	Características

Tabla 6. Amenazas o problemas identificados, que requieren atención. Fuente: Grupo de Trabajo.

La tabla 6 permite recopilar las amenazas encontradas en la etapa anterior, en relación al impacto y riesgo a que están expuestos los activos de la empresa, representados como riesgo residual e impacto residual, RR-IR (4^{ta} columna, desarrollo de procedimientos en herramienta software). Este cuadro facilitará la decisión sobre cuáles de los probables ataques serán atendidos prioritariamente, y en consecuencia, serán incluidos en la lista de problemas construida en la etapa Hacer del presente proceso.

Alineación Estrategia (AE): Como enfoque del modelo, constituye el eje central del proceso a seguir (ver figura 27). Se debe alinear las metas del negocio con los objetivos de seguridad informática que se estipulen. Así, la AE consiste en tener presente ese plan de negocio de la empresa al momento de decidir sobre la creación e implementación de una política de seguridad física, de modo que ésta contribuya a lograr los objetivos de mejor forma, sin entorpecer los procesos, contrario a eso, ayudando a fortalecerlos. En otras palabras, las medidas creadas dentro del plan de seguridad organizacional no pueden ir en contra de ciertas actividades de producción, por ejemplo. Igualmente, de ser necesario, estas tareas productivas son reformadas con la finalidad de acoplarse al cumplimiento de las políticas de seguridad física que atienden los requerimientos que guían el modelo propuesto.

En este sentido, se aplica la estrategia de alineación, haciéndose visible en la etapa 2, implementación de medidas, donde se trabajan las etapas del ciclo de vida de políticas de seguridad. De la siguiente forma:

i. Las políticas se crean de acuerdo al listado de objetos a proteger y problemas determinados en la etapa 1 del modelo de proceso.
ii. Las políticas son reformadas respecto a revisión posterior de políticas e identificación de amenazas en la etapa 3 (monitoreo), y revisión general del proceso en la etapa 4 (Actuar).
iii. A medida que se van desarrollando las políticas, se enumeran con un dígito identificador.
iv. Mediante la matriz ilustrada en la tabla 7, se establece la relación de correspondencia entre las metas del negocio y las metas de seguridad representadas en las medidas de seguridad física creadas y enumeradas anteriormente. El presente modelo propone un conjunto de metas genéricas de negocio que pueden ser ampliadas o adaptadas a la organización. la idea es plasmarlas en la tabla, y mostrar su alineación con ciertas políticas, simbolizadas a través del dígito respectivo. Adicionalmente, la matriz permite relacionar los objetivos de seguridad (tabla 8) cumplidos en ésta estrategia.

Cabe anotar que la relación existente se debe a que las políticas se van creando teniendo en cuenta las metas de la empresa que han sido preestablecidas.

	Metas del Negocio		Metas de Seguridad Informática									E2	E1	C3	I	D	C2	C1	R1	R2	R3	R4	R5	R6
Perspectiva Financiera	1	Expandir el porcentaje del mercado	8	15								x	x									x	x	
	2	Aumentar ingresos																						
	3	Retorno sobre la inversión																						
	4	Optimizar el uso de recursos																						
	5	Administrar riesgos del negocio																						
Perspectiva del Cliente	6	Mejorar orientación y servicio al cliente																						
	7	Ofrecer servicios y productos competitivos																						
	8	Disponibilidad del servicio																						
	9	Agilidad para responder requisitos cambiantes																						
	10	Optimización del costo de prestación de servicio																						
Perspectiva Interna	11	Automatizar e integrar la cadena de valor empresarial																						
	12	Mejorar y mantener la funcionalidad del proceso de negocios																						
	13	Disminuir los costos de los procesos																						
	14	Cumplimiento de leyes y reglamentos internos																						
	15	Transparencia																						
	16	Cumplimiento de políticas internas																						
	17	Mejorar y mantener la productividad operativa y del equipo de trabajo																						
Perspectiva de aprendizaje y crecimiento	18	Innovación del producto/ negocio																						
	19	Obtener información confiable y útil para la toma de decisiones																						
	20	Adquirir y mantener personal capacitado y motivado																						

Tabla 7. Matriz de alineación estratégica. Correspondencia entre metas. Fuente: Grupo de trabajo, basado en (Institute, 2005).

ID	Objetivos de Seguridad informática
C1	Confiabilidad
C2	Cumplimiento
D	Disponibilidad
I	Integridad
C3	Confiabilidad
E1	Eficiencia
E2	Efectividad

Tabla 9. Convención utilizada en la matriz para identificar objetivos de seguridad cumplidos. Fuente: Grupo de trabajo.

ID	Requisitos Fundamentales de Seguridad
R1	Política de seguridad
R2	Marcado
R3	Identificación
R4	Responsabilidad
R5	Seguridad
R6	Protección continua

Tabla 8. Convención usada en la matriz para identificar requisitos fundamentales. Fuente: Grupo de trabajo.

En la tabla 7, los números 8 y 15 que aparecen resaltados en las dos primeras columnas de las metas de seguridad, constituyen un ejemplo, que permite observar que existen dos políticas que se alinean estratégicamente a la meta de *expandir el porcentaje del mercado*, además de cumplir con los objetivos de seguridad eficiencia y efectividad, referenciados en la tabla 8.

Los requisitos fundamentales de seguridad, como se aprecia en la estructura diseñada (figura 27), son controles que evaluarán el desempeño del esquema de seguridad. Controles que brindan ciertas pautas[13] a cumplir en las etapas del plan de seguridad, específicamente en la fase 2, implementación de las políticas, es allí donde el(los) encargado(s) deberá(n) hacer visibles tres aspectos: Política (política de seguridad, marcado), Responsabilidad (identificación, responsabilidad) y Garantía (seguridad, protección continua), que se traducen en (6) seis requisitos fundamentales para considerar un sistema seguro (de acuerdo a RFC 2196).

La evaluación del cumplimiento de estos requisitos está incluida en la matriz de alineación estratégica (tabla 7), las últimas seis columnas permiten inspeccionar la atención que dan las políticas de seguridad física relacionadas en ese registro a los controles, que están representados por identificadores (R1-R6) precisados en la tabla 9. En el ejemplo presentado, suponemos que las políticas 8 y 15 atienden los requisitos *seguridad* y *marcado.*

En este orden, la matriz permite realizar una relación completa de correspondencia entre: Metas del negocio, Metas de Seguridad informática (representadas en las políticas de seguridad física) Objetivos de seguridad informática y los Requisitos fundamentales de seguridad, como controles del modelo EBASF.

NOTA: El desarrollo del proceso descrito en este apartado, se podrá observar de forma amplia en la herramienta software que se encuentra anexa al presente documento, en medio magnético (CD).

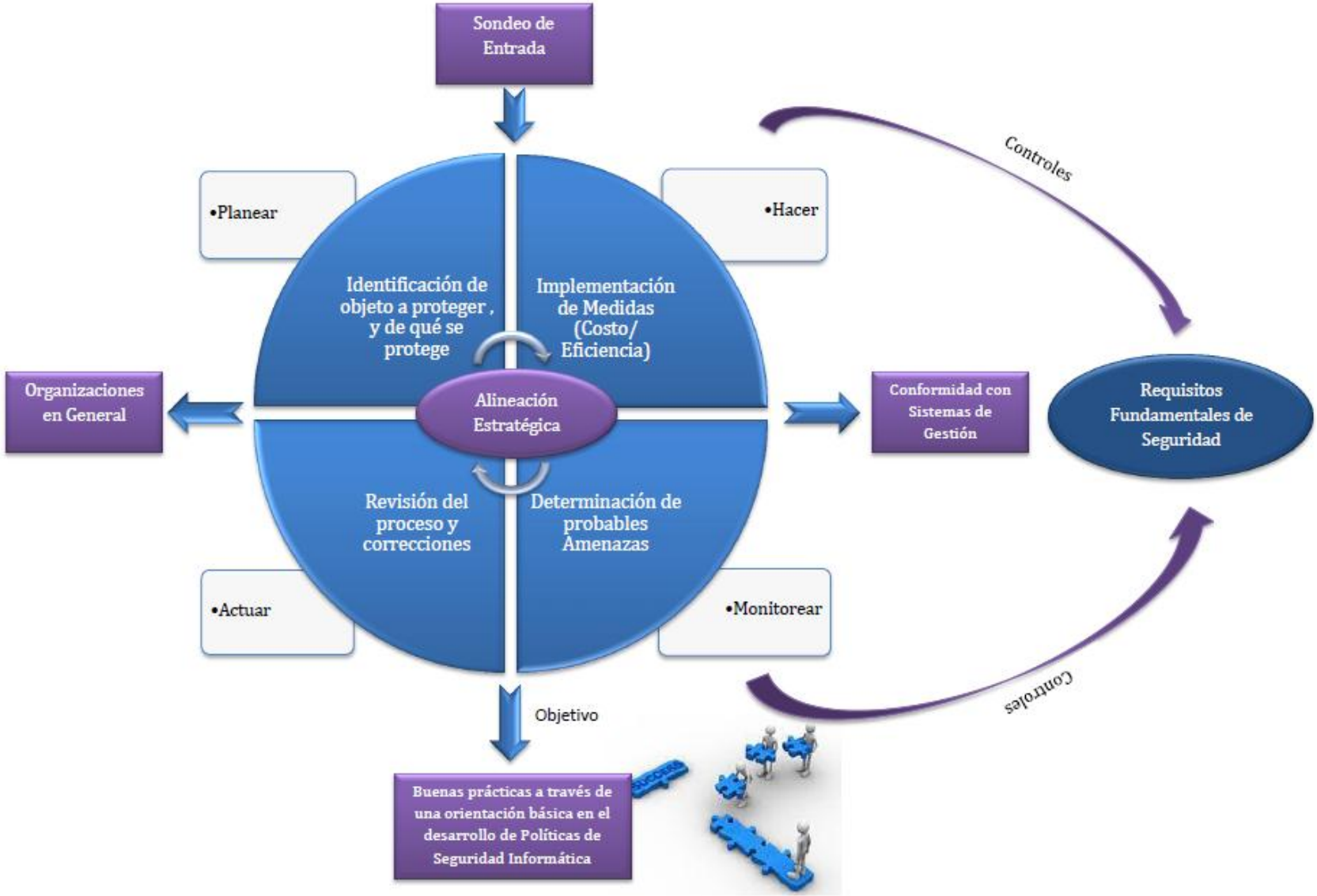


Figura 27. Estructura del Modelo de Seguridad Informática EBASF, diseñado como resultado final del proceso. Fuente: Grupo de Trabajo.

6. ARQUITECTURA DEL MODELO EBASF MATERIALIZADO EN LA HERRAMIENTA SOFTWARE DE APOYO AL PROCESO

A partir de la estructuración del Esquema Básico de Seguridad Física (EBASF), en este capítulo se construye la arquitectura del software que corresponde a la implementación del mismo, a través de modelos se representan las funcionalidades de la herramienta, siguiendo el modelo 4+1 vistas, como se desarrolla a continuación.

6.1. VISTA LÓGICA

Mediante el diagrama de clases se ilustra la arquitectura lógica del sistema, que permite atender los requisitos funcionales del sistema, esto es, lo que el sistema debe brindar a los usuarios en términos de servicios.

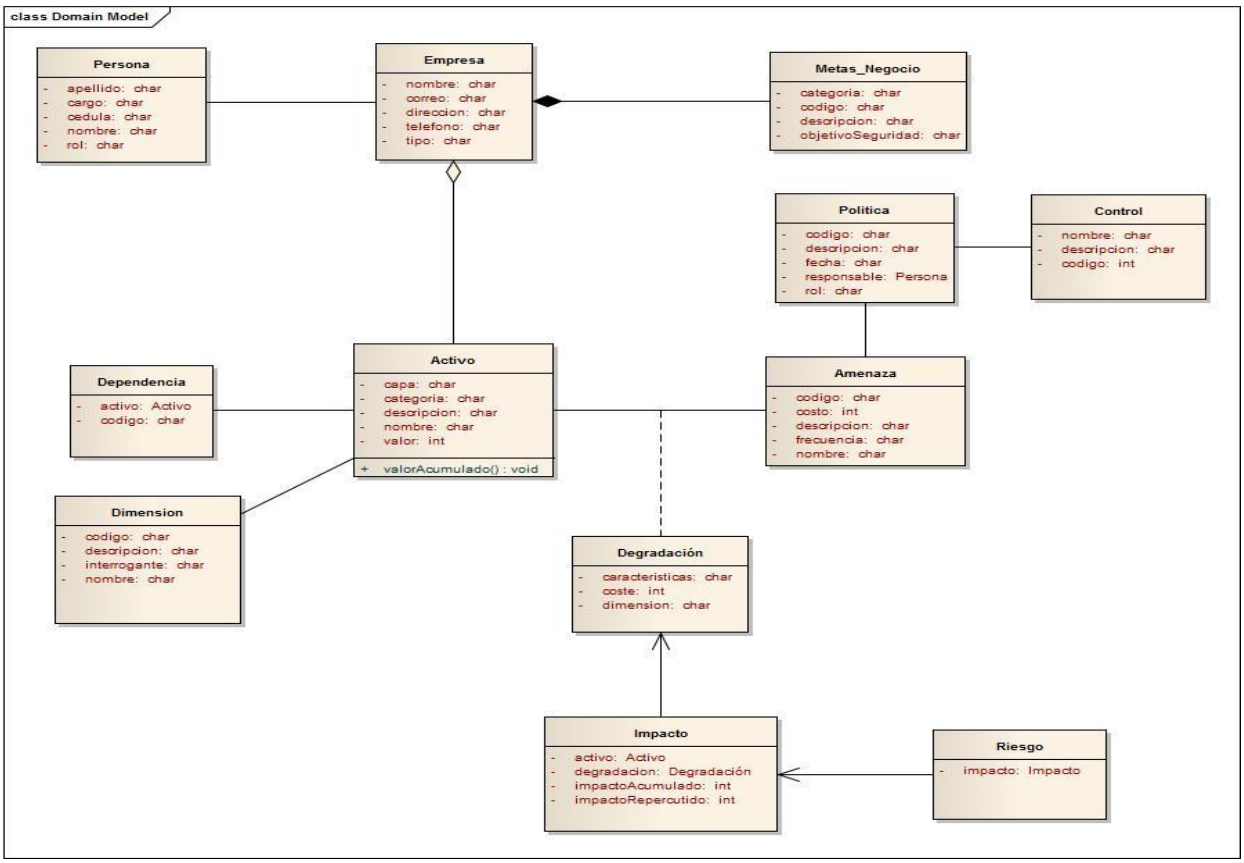


Figura 28. Arquitectura lógica del sistema. Fuente: Grupo de Trabajo.

6.2. VISTA DE PROCESOS

El modelo permite ilustrar cómo interactúan las clases identificadas en la vista lógica y la secuencia de comunicación entre procesos, que evidencian el cumplimiento de los requerimientos del sistema.

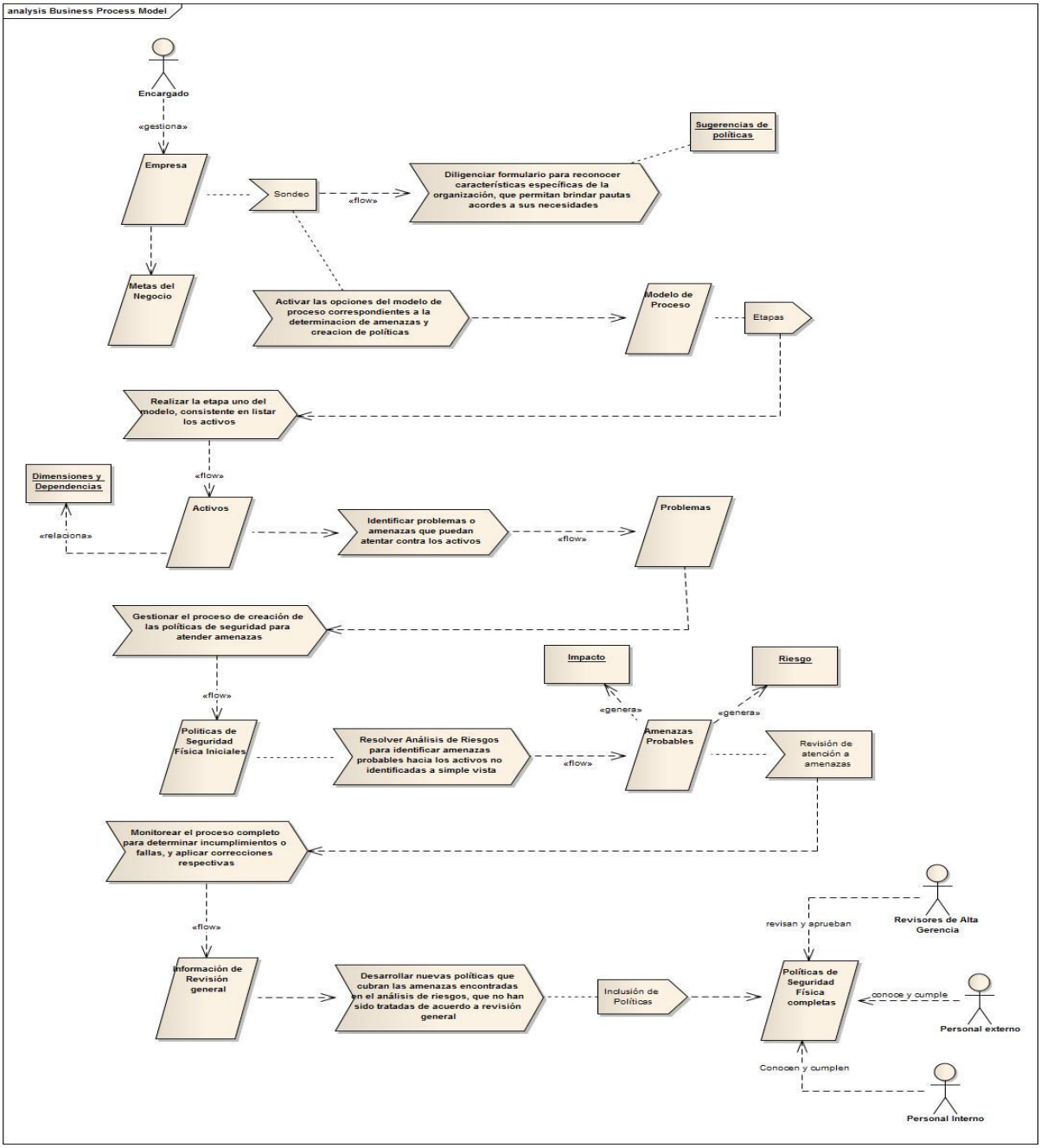


Figura 29. Ilustración de la secuencia de procesos. Fuente: Grupo de Trabajo.

6.3. VISTA DE DESARROLLO

Esta vista se centra en la organización real de los módulos de software en el ambiente de desarrollo del software. El sistema se empaqueta en partes pequeñas que pueden ser desarrolladas y tratadas de forma independiente. Los subsistemas se organizan en una jerarquía de capas relacionadas, que en el siguiente diagrama evidencian la aplicación del Modelo Vista Controlador, MVC, para brindar una estructura organizada a nivel de programación.

El componente Modelo, comprende las clases que manejan una serie de procesos lógicos que dan lugar a las funcionalidades del software. La Vista es el componente que maneja las interfaces que se muestran al usuario, encargándose de publicar los diferentes elementos visuales que éste necesita para acceder y manejar las opciones del software. El Controlador contiene las clases de intercesión entre la vista y el modelo, donde los datos son recibidos, verificados y enviados a cumplir su función.

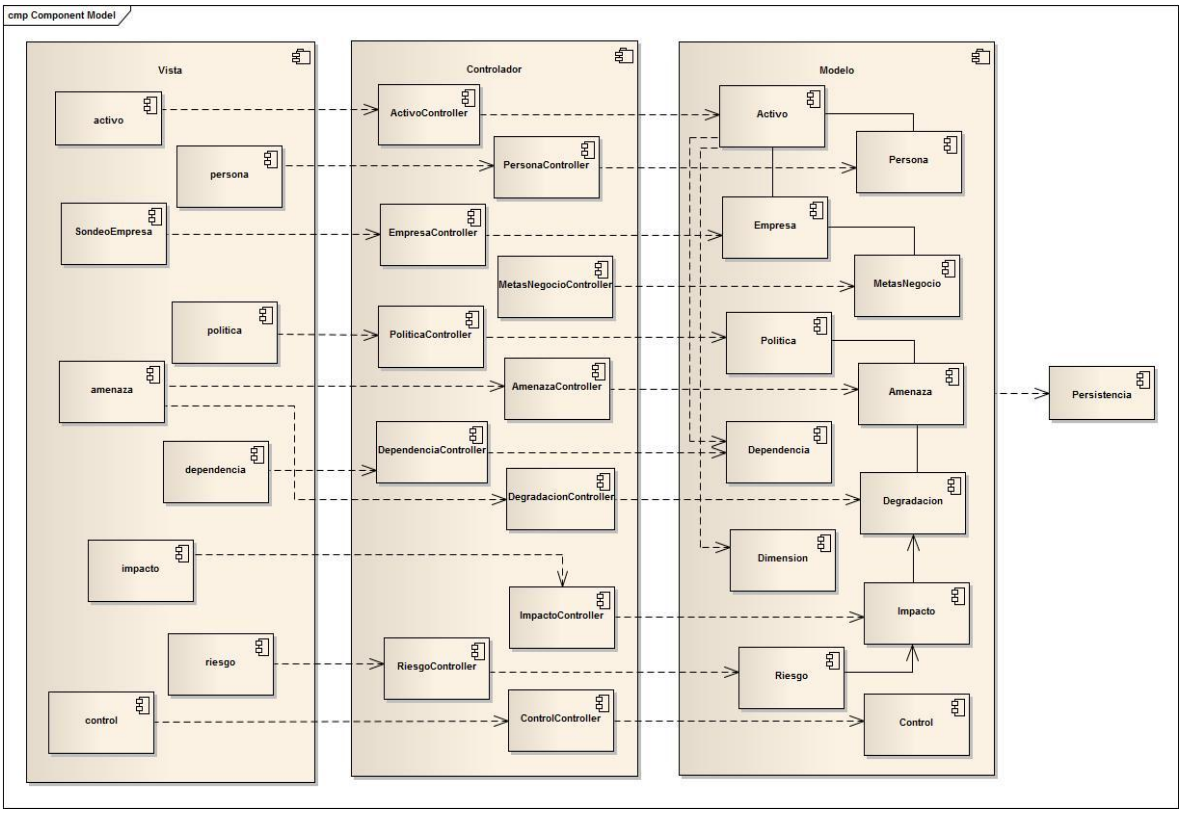


Figura 30. Diagrama de componentes. Fuente: Grupo de Trabajo.

6.4. VISTA FÍSICA

La arquitectura física permite mostrar la interacción de los componentes con equipos, servicios, plataformas, entre otros.

El sistema EBASF se despliega sobre un servidor de aplicaciones, que se conecta al servidor de base de datos MySQL.

El usuario de la aplicación puede acceder a ella a través de internet, mediante un navegador o browsers.

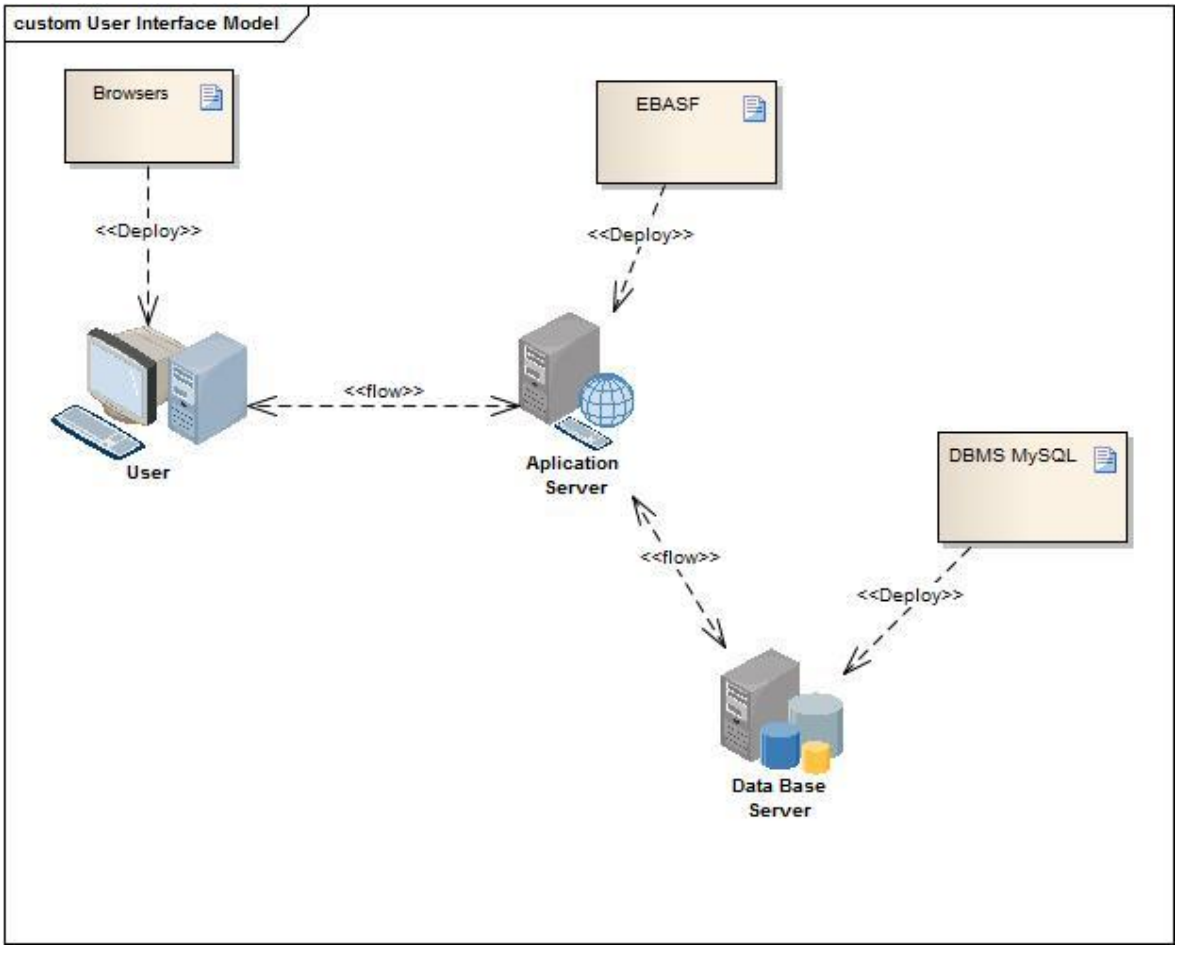


Figura 31. Muestra el despliegue físico del sistema. Fuente: Grupo de Trabajo.

6.5. VISTA DE ESCENARIOS

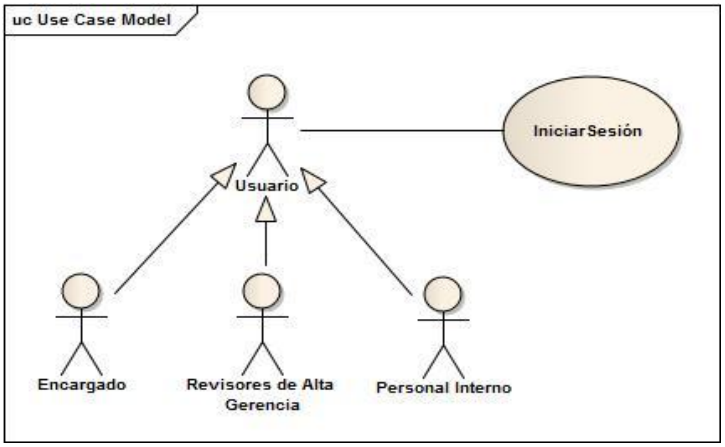


Figura 32. Caso de uso iniciar sesión. Fuente: Grupo de Trabajo.

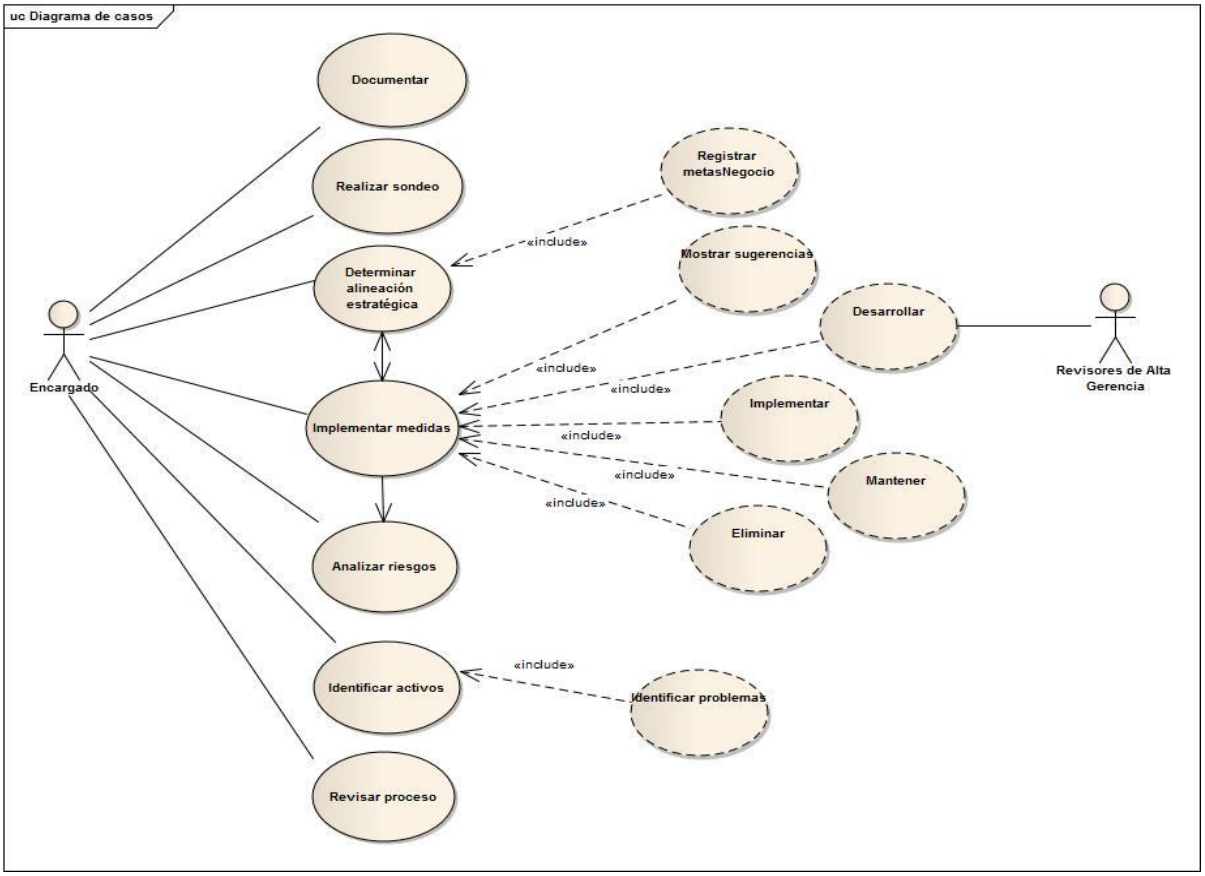


Figura 33. Funcionalidades del sistema dentro de un escenario de aplicación. Fuente: Grupo de Trabajo.

7. PROCESO DE CREACIÓN DE POLÍTICAS DE SEGURIDAD FÍSICA COMO PRUEBA, BASADA EN EL ESQUEMA DESARROLLADO: AKENDOS S.A.S

7.1. GENERALIDADES DE LA PRUEBA

Culminado el proyecto investigativo "Software de Apoyo al proceso de Creación y Registro de Políticas de Seguridad Informática en Organizaciones", se procede a realizar una prueba del modelo diseñado a través del uso de la aplicación por parte de un funcionario asignado por la empresa de desarrollo software **Akendos S.A.S**, como escenario seleccionado para ello, por ser una compañía que carece de esquemas o controles de seguridad informática, además de contar con el personal con los conocimientos mínimos requeridos para el uso del aplicativo. La actividad consiste en explicarle al funcionario los objetivos y funcionalidades del sistema para que continúe con el ingreso y familiarización. Luego, éste sigue las sugerencias y de acuerdo a los requerimientos de la empresa, crea las primeras políticas de seguridad física, haciendo los registros respectivos.

Al finalizar, expone la experiencia y su posición frente a la utilidad de la herramienta. Es preciso aclarar que el modelo y sistema software está delimitado a la creación adecuada de las políticas, saliéndose de su alcance la implantación, cumplimiento y garantía de éxito en la organización, pues ello depende factores como la concienciación y compromiso del recurso humano, la disposición de herramientas, manejo adecuado de la guía, entre otros.

7.2. DESCRIPCIÓN DEL ESCENARIO DE PRUEBA

Akendos S.A.S. es una compañía de desarrollo software ubicada en una zona residencial de la ciudad de Cartagena, Colombia; a nivel de infraestructura está integrada por un centro de desarrollo, una oficina de atención y una zona de juegos. Actualmente, en el escenario no hay políticas definidas, ni en desarrollo, lo que conlleva a realizar el proceso sin referencias a antecedentes. La gerencia está a cargo del ingeniero Giovanny Sayas Acevedo, quién cumplirá el rol de usuario del sistema como Consultor en la actividad de prueba, dado que cuenta con los conocimientos mínimos requeridos.

7.3. PRAXIS DEL PROCESO

La aplicación web EBASF, despliega la interfaz que ilustra la imagen 34. El usuario en su rol de Consultor (denominado también encargado, en el desarrollo del documento) del proceso de creación de las primeras políticas de seguridad física, ingresa a la aplicación con el *users* y *password* asignados.

Figura 34. Interfaz inicial de ingreso a la aplicación. Fuente: Grupo de Trabajo.

Revisada la documentación necesaria brindada por el sistema, se procede a realizar el Sondeo Inicial (ver figura 35). Una vez finalizado se da paso hacia el desarrollo del Modelo de proceso, que inicia con la etapa **Planear**; el encargado lista los activos, tal como indica la herramienta, siguiendo la nomenclatura y pautas ofrecidas (figura 36).

Figura 35. Ventana de Sondeo Inicial realizado antes de las etapas del modelo.

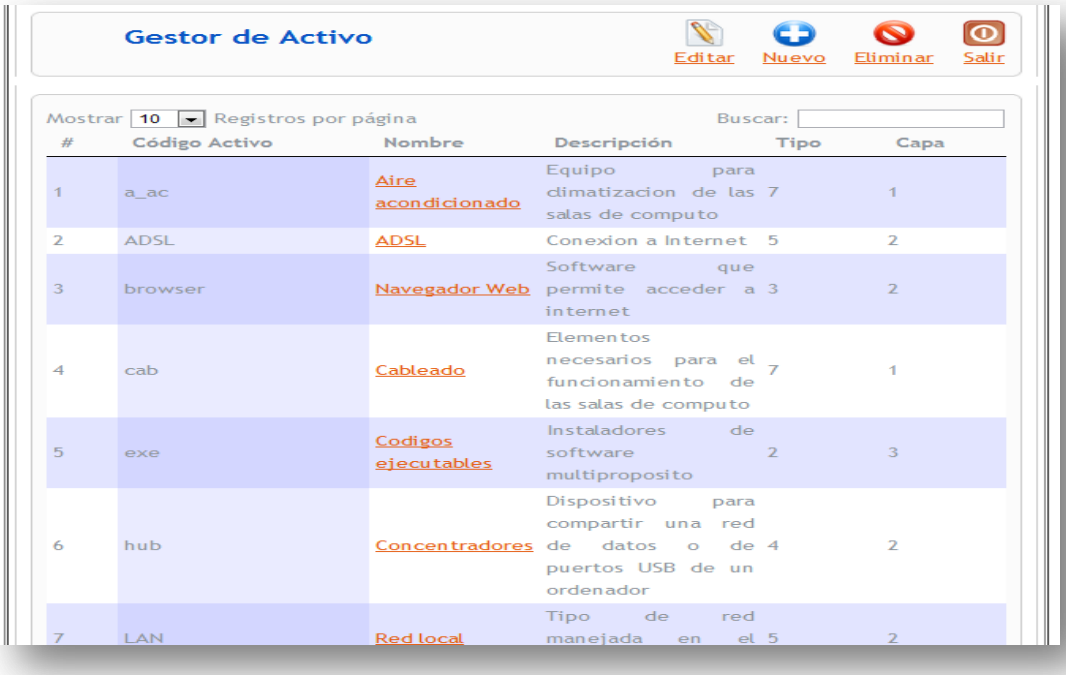


Figura 36. Registro de activos identificados en el escenario de prueba.

El encargado listó igualmente los problemas más comunes que observa en el centro de cómputo, relacionados con incidentes de seguridad. Luego, la etapa siguiente, **Hacer**, consta de la implementación de las medidas siguiendo el denominado Ciclo de vida. El consultor se documenta y procede a redactar las políticas de seguridad física que considera cubren los problemas registrados. El sistema despliega 3 fundamentos que se deben estudiar antes de diseñarlas (Figuras 37).

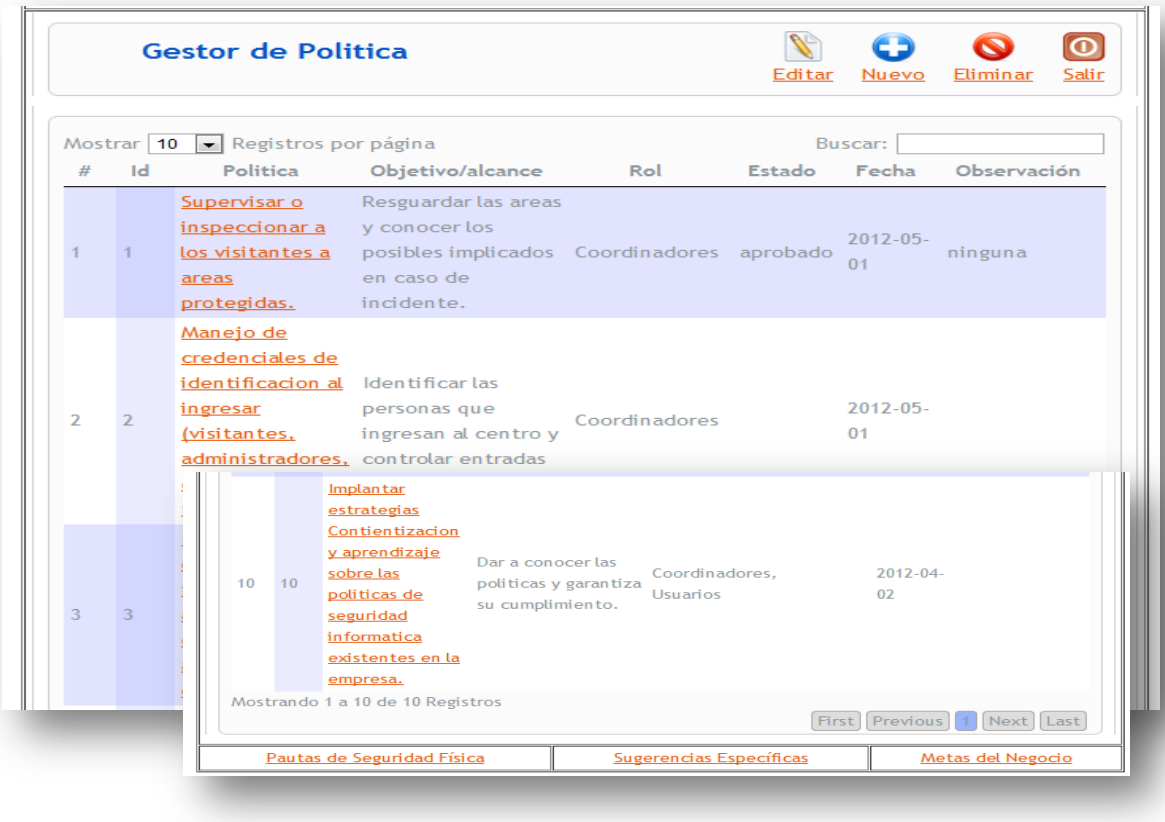
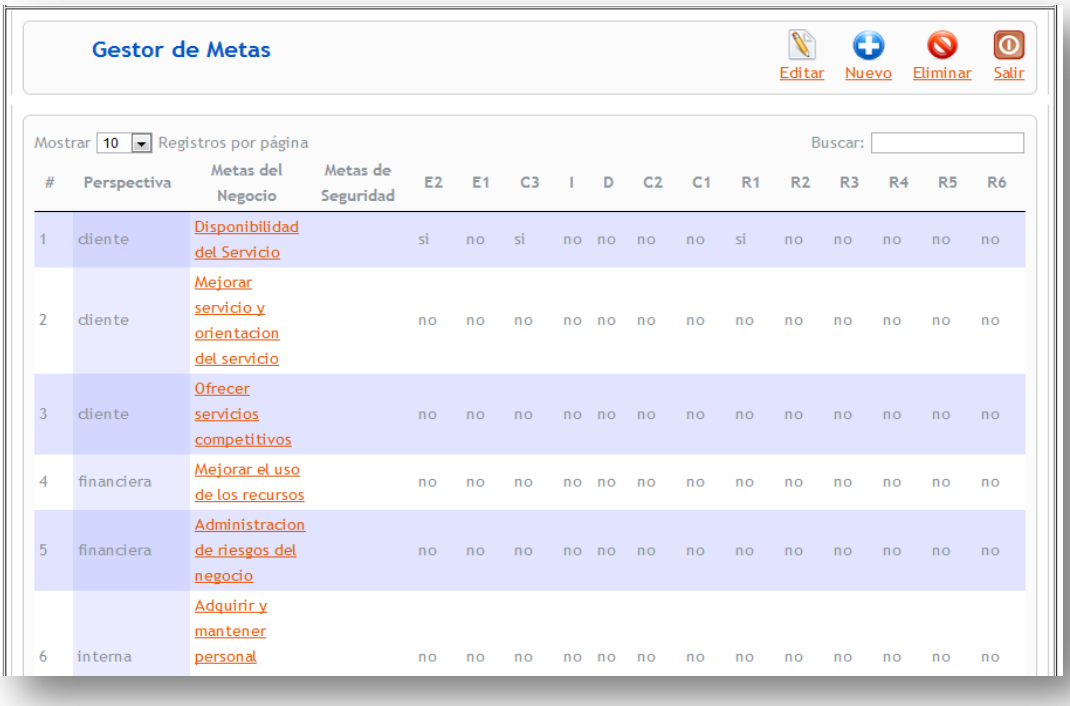


Figura 37. Tabla que permite registrar, añadir, modificar, y eliminar las políticas.

La imagen 38 muestra la forma en que se despliega una de las ayudas al usuario en la creación de las políticas.



#	Perspectiva	Metas del Negocio	Metas de Seguridad	E2	E1	C3	I	D	C2	C1	R1	R2	R3	R4	R5	R6
1	cliente	Disponibilidad del Servicio		si	no	si	no	no	no	no	si	no	no	no	no	no
2	cliente	Mejorar servicio y orientacion del servicio		no	no	no	no	no	no	no	no	no	no	no	no	no
3	cliente	Ofrecer servicios competitivos		no	no	no	no	no	no	no	no	no	no	no	no	no
4	financiera	Mejorar el uso de los recursos		no	no	no	no	no	no	no	no	no	no	no	no	no
5	financiera	Administracion de riesgos del negocio		no	no	no	no	no	no	no	no	no	no	no	no	no
6	interna	Adquirir y mantener personal		no	no	no	no	no	no	no	no	no	no	no	no	no

Figura 38. Metas del negocio, que debe tener en cuenta el encargado.

Las etapas de Implementación, Mantenimiento y Eliminación del ciclo de vida, se obvian en este recorrido, debido a que es el primero, y las políticas hasta este punto aún no se han finalizado ni implementado. De esta forma, se continúa con la etapa **Monitorear** del modelo; El sistema muestra una opción <<MAGERIT 2.0>> y otra <<Iniciar Análisis de Riesgos>>, dado que la primera es el documento oficial de la metodología de análisis de riesgos a desarrollar, se sigue hacia la segunda opción que despliega el menú de la misma (Figura 39).

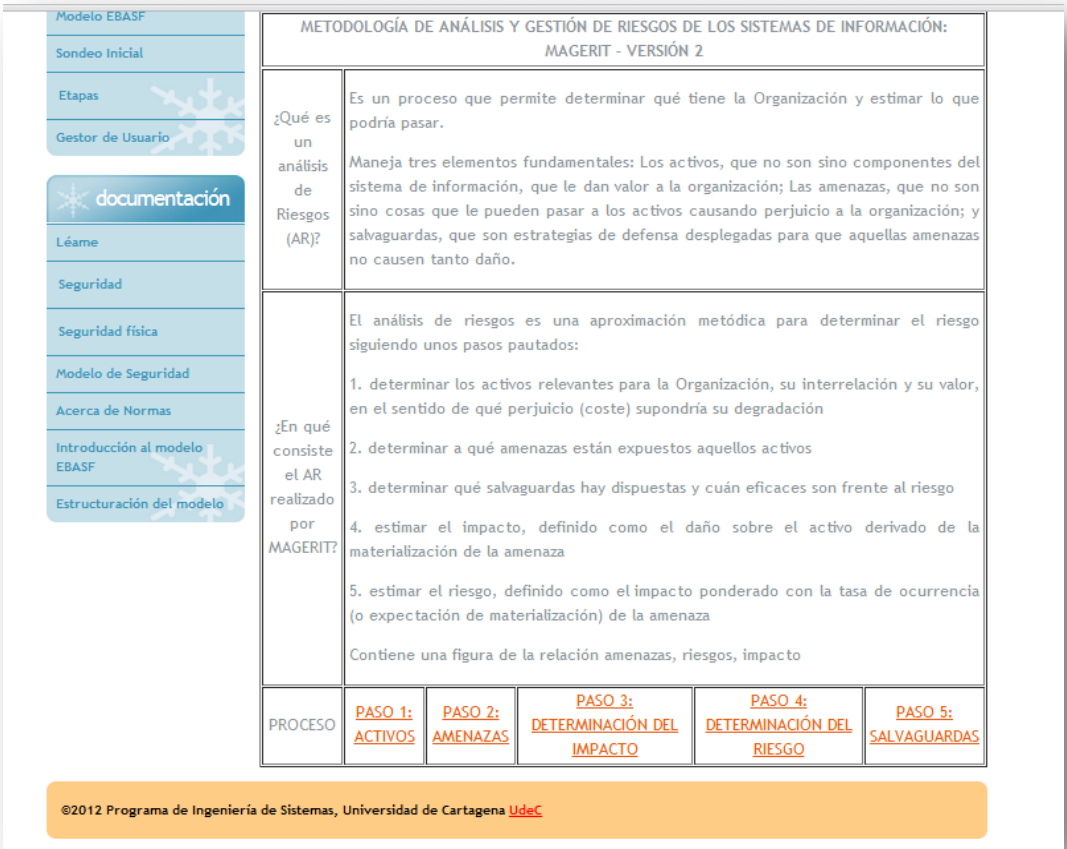


Figura 39. Menú de opciones de MAGERIT 2.0, que describe los pasos a realizar.

El encargado ingresa al paso 1, donde se le muestra la lista de activos registrados; él estipula la relación de Dependencia entre éstos, teniendo en cuenta cuáles son inferiores y superiores, y de acuerdo a las capas, como le es señalado en el software (Figura 40).

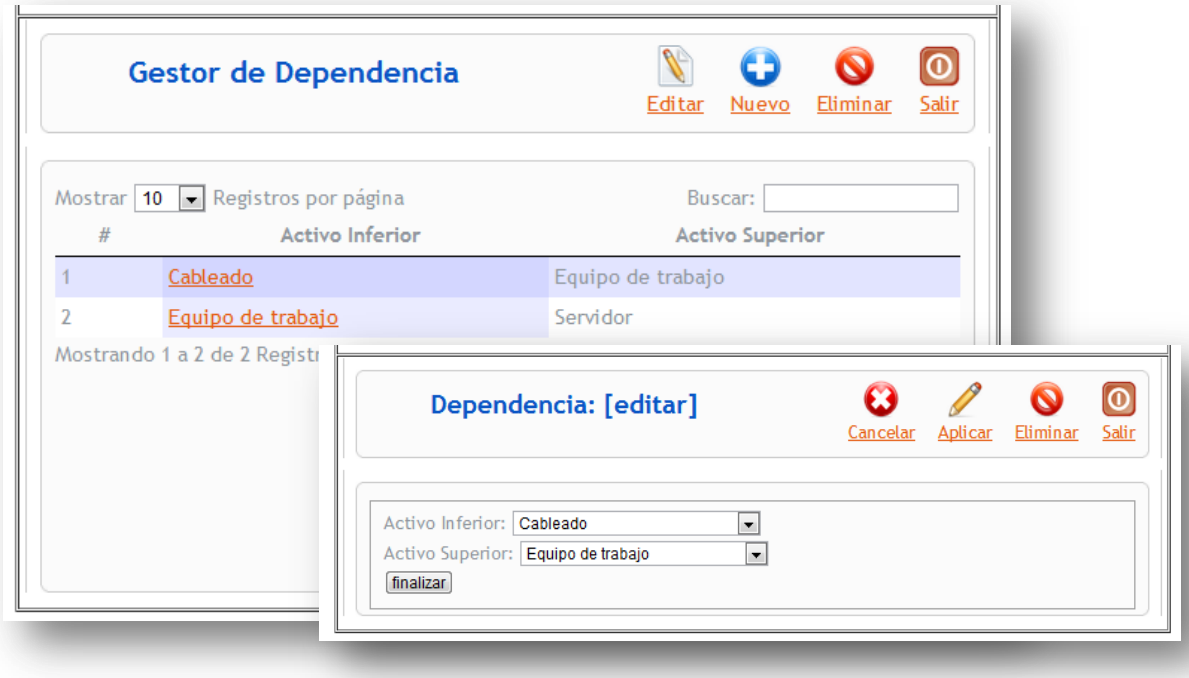


Figura 40. Determinación de relación de dependencia entre activos.

Seguidamente, el consultor asigna un Valor propio a cada activo en sus *dimensiones*, fundamentado en las sugerencias brindadas y la Escala estándar desplegada. Mientras que el software calcula y da la opción de mostrar el Valor acumulado (Figura 41).

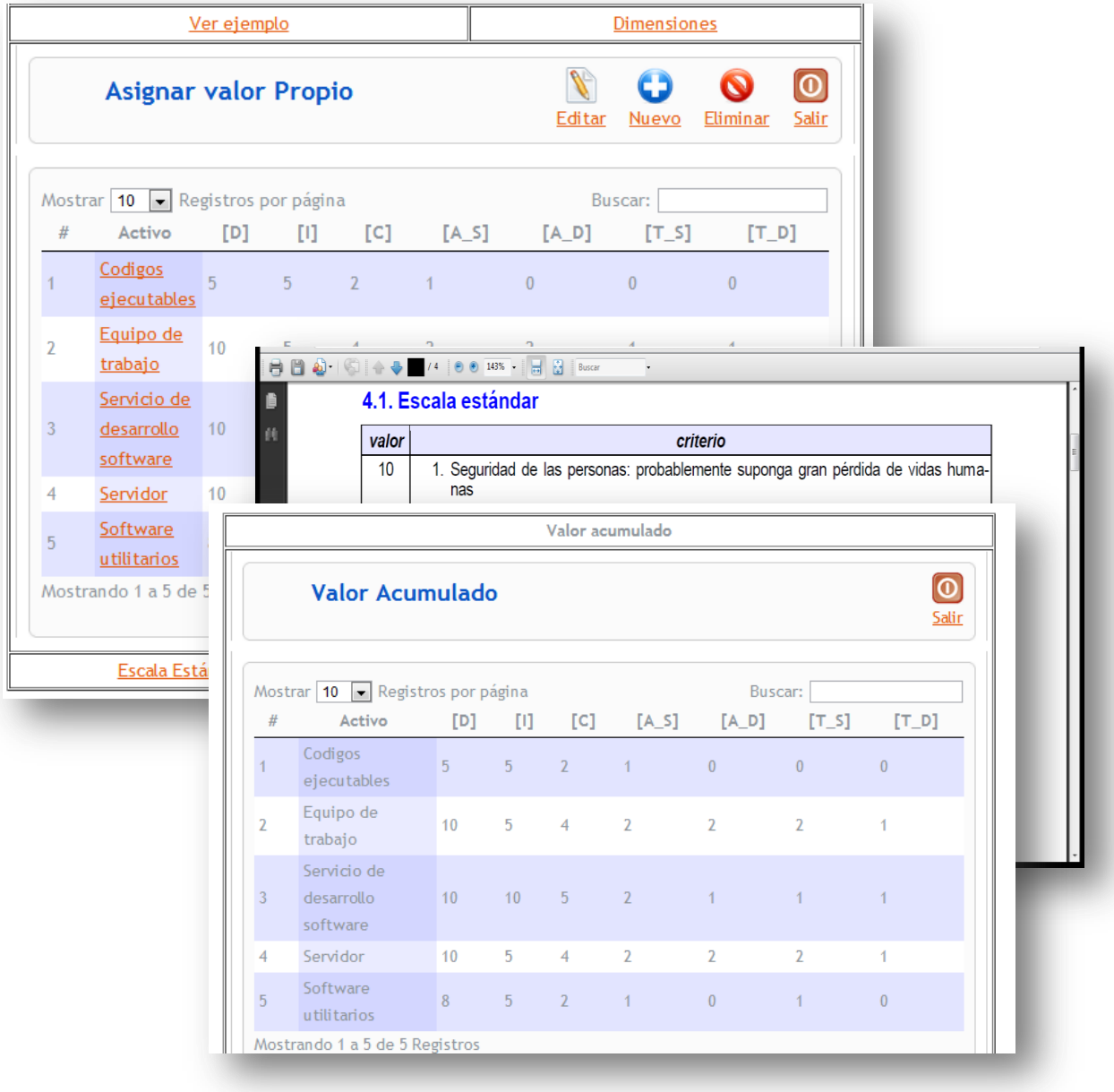
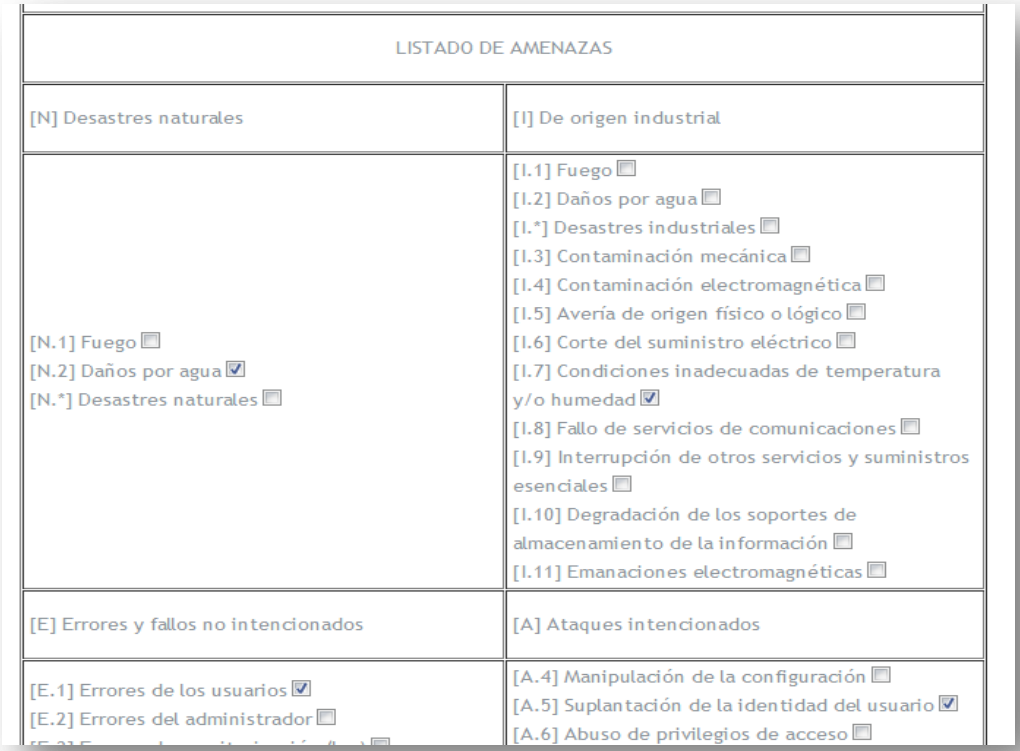


Figura 41. Asignación de Valor propio. Despliegue de Escala estándar de valoración. Cálculo del Valor acumulado de cada activo.

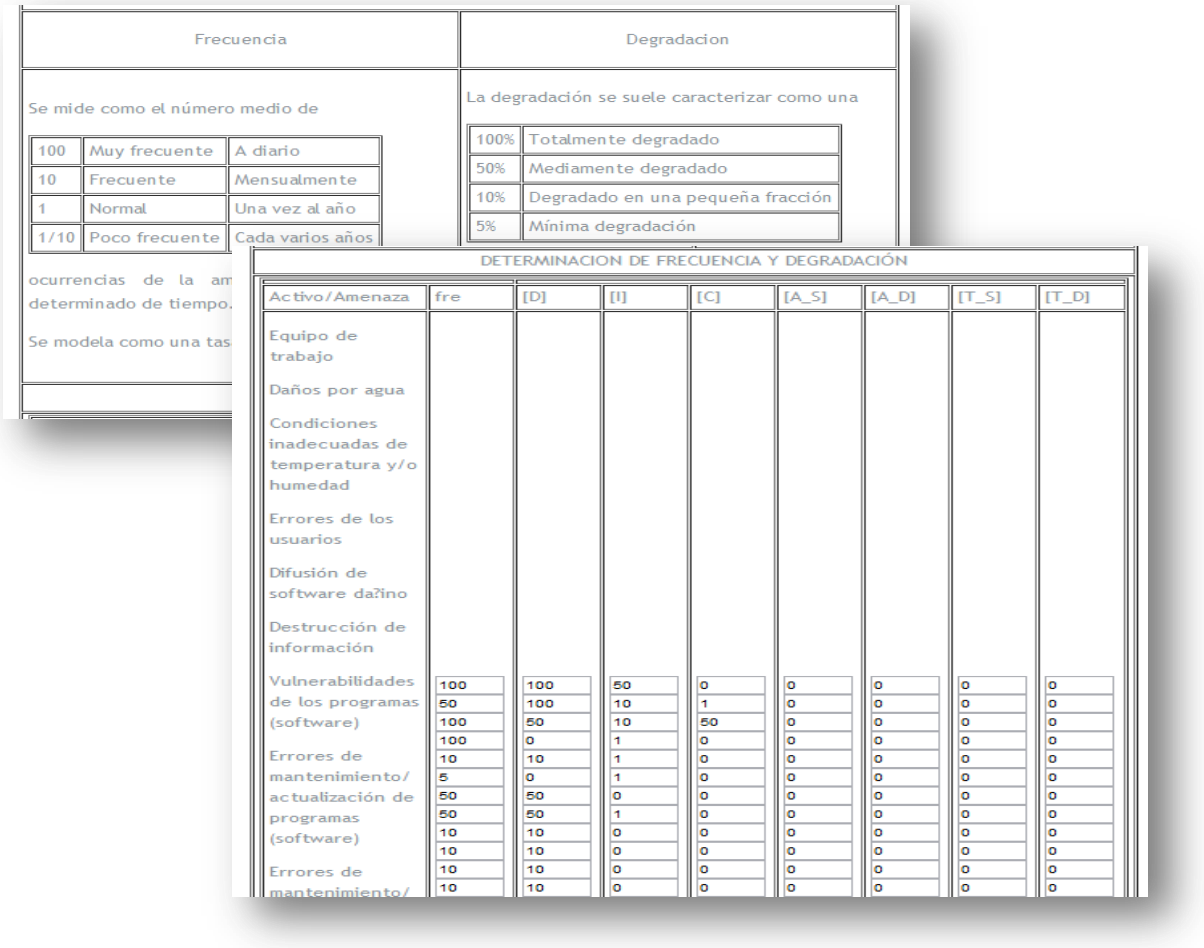
Luego, en el paso 2, el encargado selecciona de la lista de amenazas MAGERIT, las que considera pueden afectar los activos del centro de cómputo, teniendo como precedente que ya identificó problemas, y en este punto debe contemplar amenazas probables (figura 42). Se apoya en el catálogo de amenazas presentado.



LISTADO DE AMENAZAS	
[N] Desastres naturales	[I] De origen industrial
[N.1] Fuego ☐ [N.2] Daños por agua ☑ [N.*] Desastres naturales ☐	[I.1] Fuego ☐ [I.2] Daños por agua ☐ [I.*] Desastres industriales ☐ [I.3] Contaminación mecánica ☐ [I.4] Contaminación electromagnética ☐ [I.5] Avería de origen físico o lógico ☐ [I.6] Corte del suministro eléctrico ☐ [I.7] Condiciones inadecuadas de temperatura y/o humedad ☑ [I.8] Fallo de servicios de comunicaciones ☐ [I.9] Interrupción de otros servicios y suministros esenciales ☐ [I.10] Degradación de los soportes de almacenamiento de la información ☐ [I.11] Emanaciones electromagnéticas ☐
[E] Errores y fallos no intencionados	[A] Ataques intencionados
[E.1] Errores de los usuarios ☑ [E.2] Errores del administrador ☐	[A.4] Manipulación de la configuración ☐ [A.5] Suplantación de la identidad del usuario ☑ [A.6] Abuso de privilegios de acceso ☐

Figura 42. Registro de amenazas que podrían llegar a atentar contra los activos registrados y valorados en etapa anterior.

El encargado relaciona estas amenazas con los activos que son afectados. Así mismo, asigna un valor de Degradación y Frecuencia de las amenazas sobre los activos. La asignación de valores la realiza con base en las escalas mostradas (Figura 43)



Frecuencia		
Se mide como el número medio de		
100	Muy frecuente	A diario
10	Frecuente	Mensualmente
1	Normal	Una vez al año
1/10	Poco frecuente	Cada varios años
ocurrencias de la am		
determinado de tiempo.		
Se modela como una tas		

Degradacion	
La degradación se suele caracterizar como una	
100%	Totalmente degradado
50%	Mediamente degradado
10%	Degradado en una pequeña fracción
5%	Mínima degradación

DETERMINACION DE FRECUENCIA Y DEGRADACIÓN

Activo/Amenaza	fre	[D]	[I]	[C]	[A_S]	[A_D]	[T_S]	[T_D]
Equipo de trabajo								
Daños por agua								
Condiciones inadecuadas de temperatura y/o humedad								
Errores de los usuarios								
Difusión de software dañino								
Destrucción de información								
Vulnerabilidades de los programas (software)	100	100	50	0	0	0	0	0
	50	100	10	1	0	0	0	0
	100	50	10	50	0	0	0	0
Errores de mantenimiento/ actualización de programas (software)	100	0	1	0	0	0	0	0
	10	10	1	0	0	0	0	0
	5	0	1	0	0	0	0	0
	50	50	0	0	0	0	0	0
	50	50	1	0	0	0	0	0
	10	10	0	0	0	0	0	0
	10	10	0	0	0	0	0	0
Errores de mantenimiento/	10	10	0	0	0	0	0	0
	10	10	0	0	0	0	0	0

Figura 43. Asignación de Frecuencia y Degradación causada por cada amenaza sobre cada actico afectado, en cada una de sus dimensiones.

El Consultor realiza los pasos 4 y 5, que corresponden a la determinación de impacto y riesgo que realiza el sistema con base a los datos hasta ese momento registrados. Se le muestra el Impacto y Riesgo, acumulado y repercutido que cada probable amenaza causa sobre cada dimensión de un activo (Figura 44).

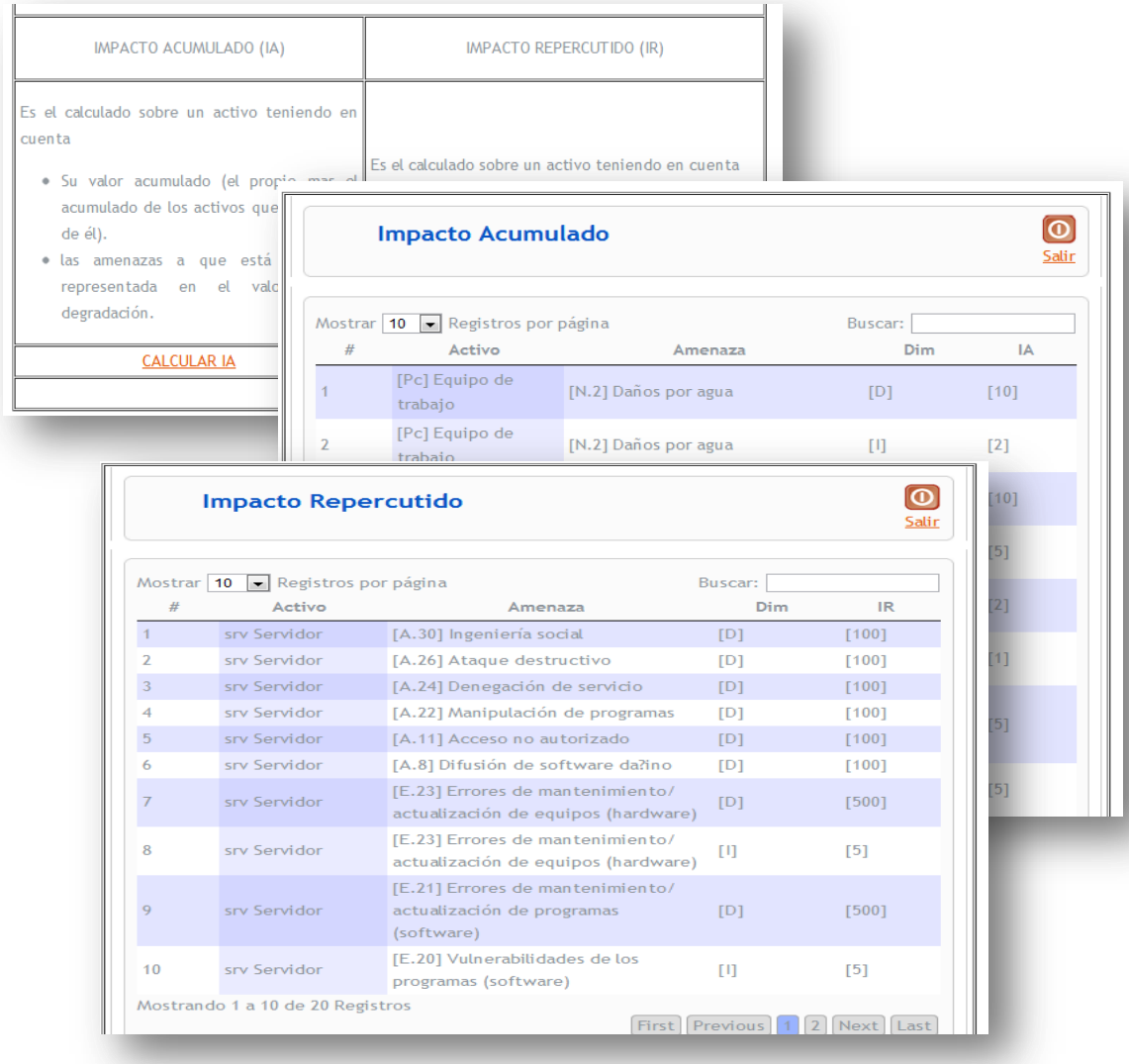
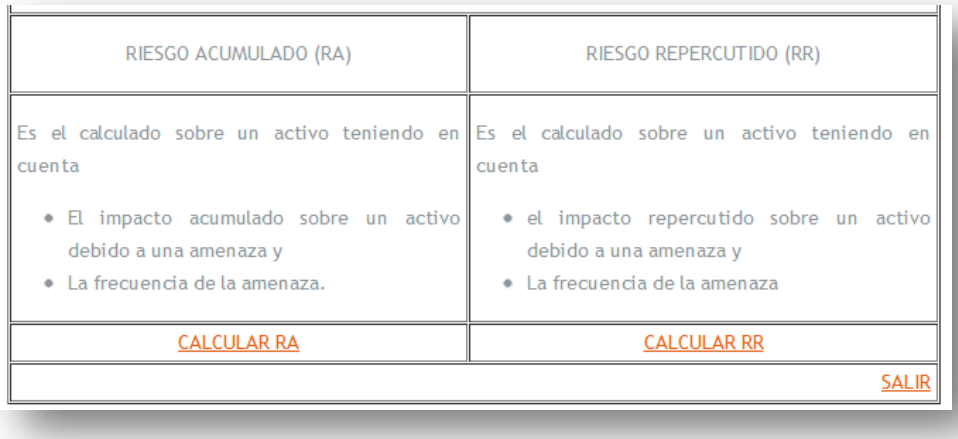


Figura 44. Ventanas de valores del Impacto acumulado e Impacto repercutido.



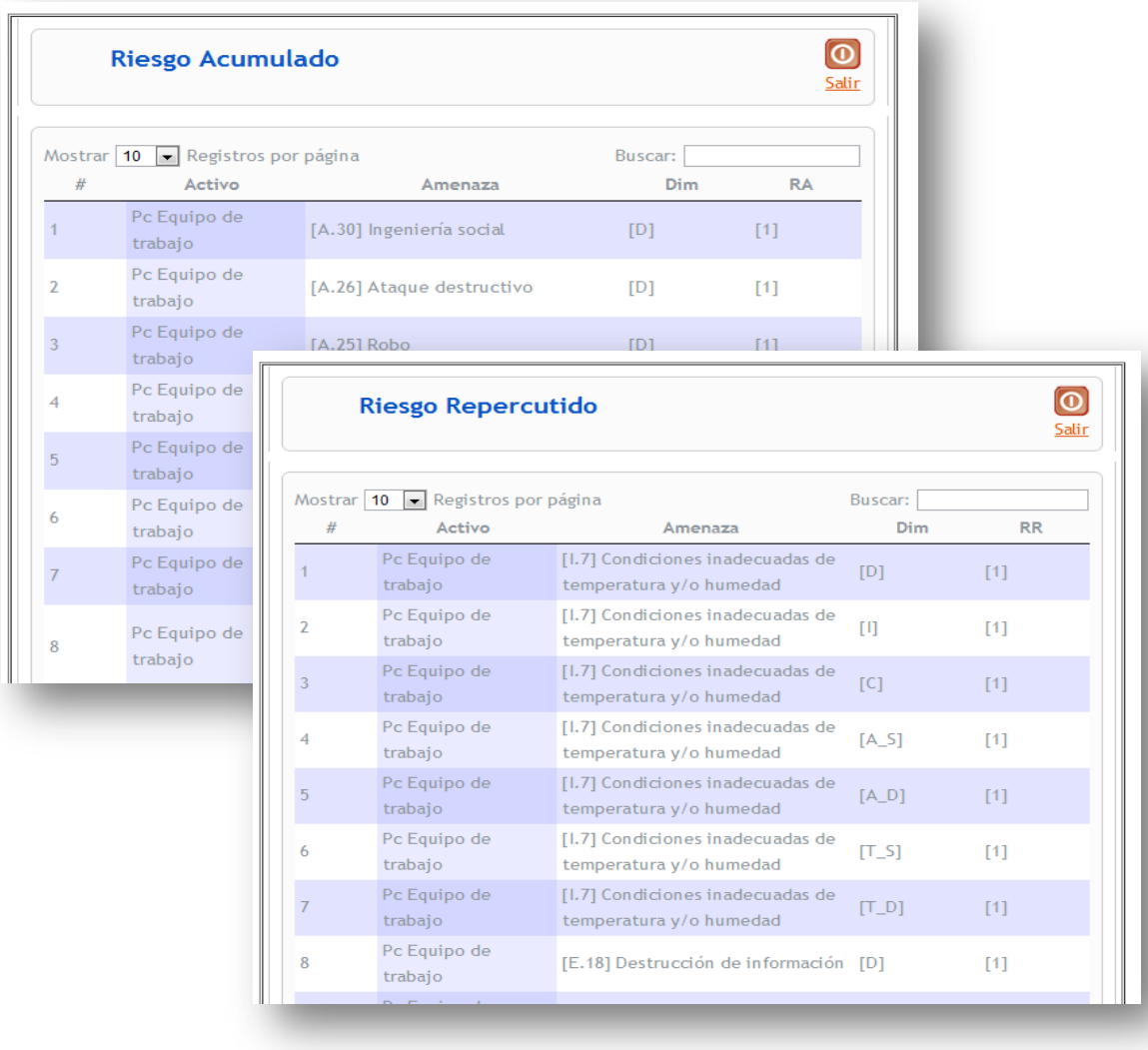


Figura 45. Ventana de valores del Riesgo acumulado.

Con la información suministrada por las tablas como la mostrada en las figuras 44 y 45, el encargado tiene bases para tomar medidas que atiendan las amenazas de riesgo e impacto más alto, de acuerdo a los valores. Sin embargo, él completa el modelo de proceso en la etapa **Actuar**. Aquí el encargado, realiza una revisión general del proceso, a través del cuadro mostrado en la figura 46.

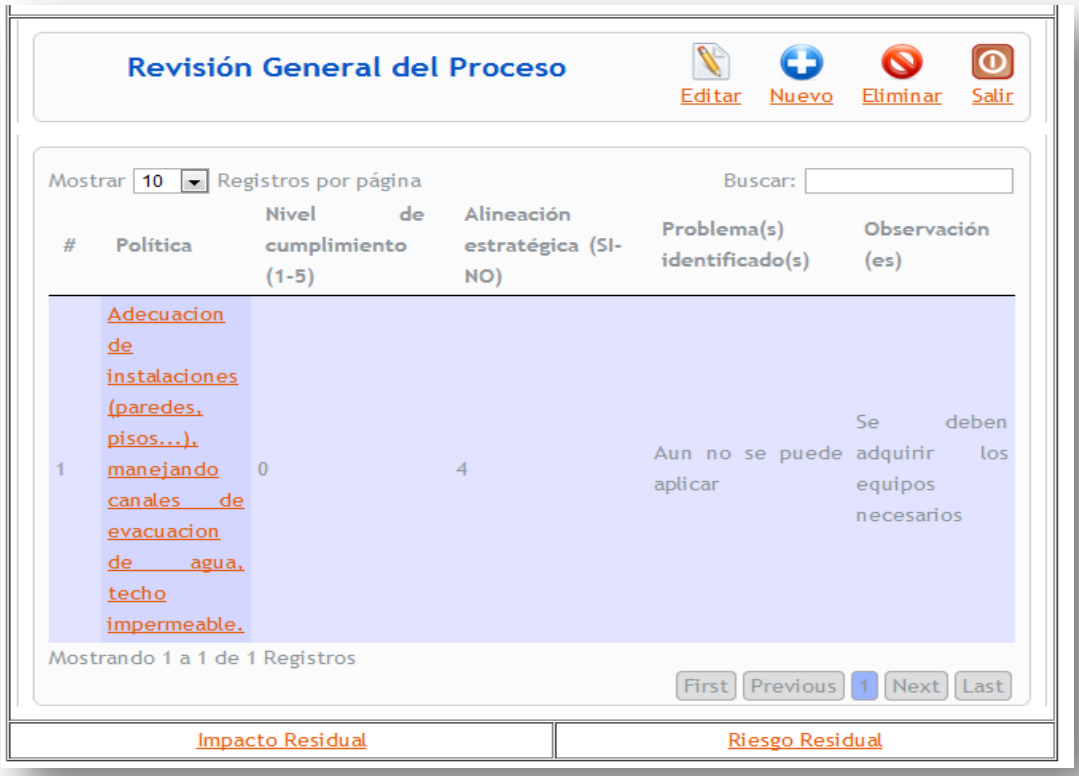


Figura 46. Revisión General realizada a todo el proceso que se tiene hasta el momento.

Además, accede a la opción que le permite visualizar la tabla depurada de amenazas que requieren atención inmediata (figura 47).

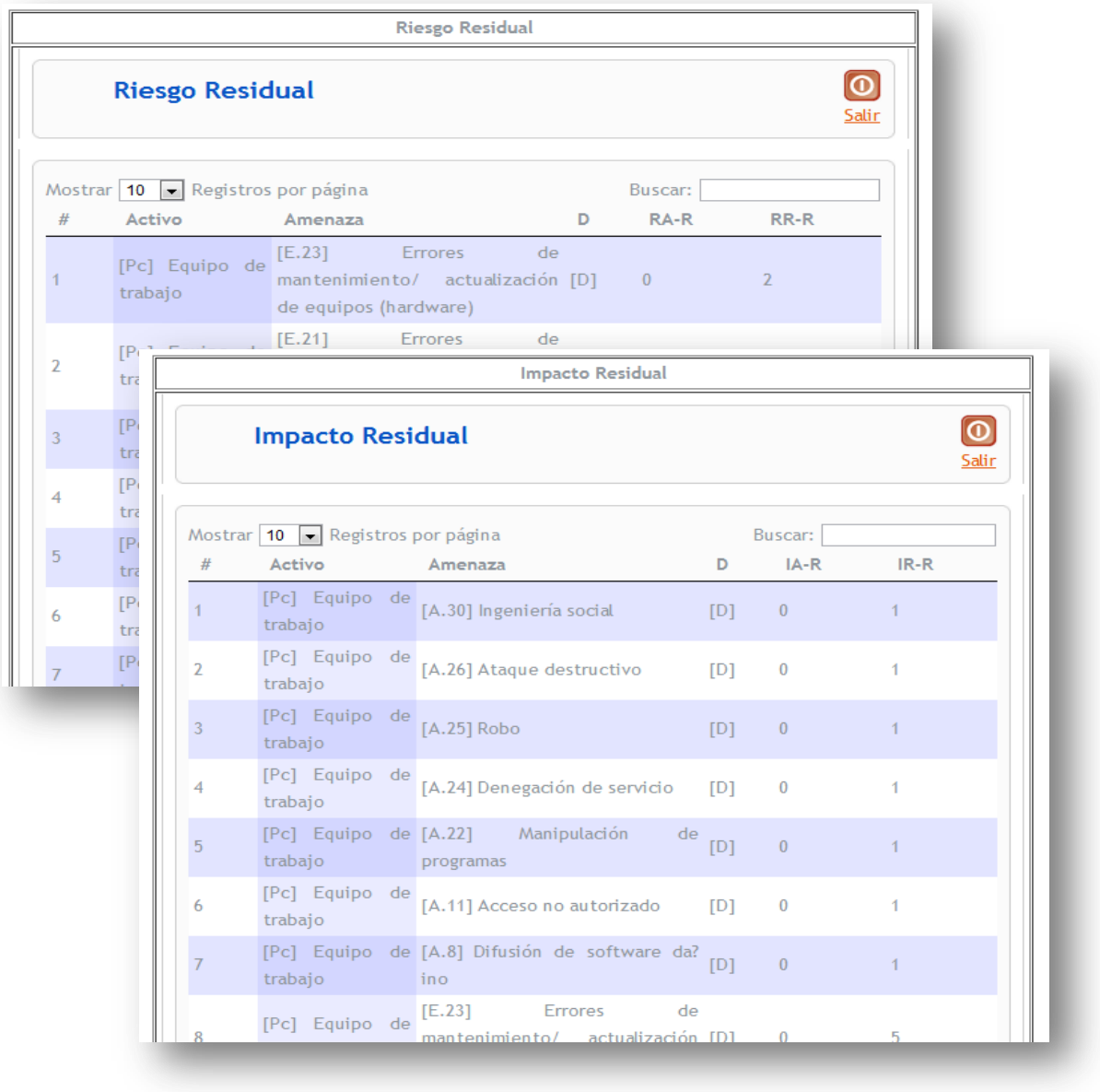


Figura 47. Valores de Riesgo e Impacto residual generados como resultados finales del proceso.

Con esta información el consultor, gerente de Akendos, puede reiniciar el ciclo de trabajo para incluir las políticas necesarias que le permitan reducir los riesgos a problemas encontrados. Sin embargo, por lo extendido del proceso, la prueba se realiza hasta este punto; donde pudo conocer la herramienta y hacer uso de ella en la creación de las políticas

iniciales del centro de la empresa, determinando los riesgos a amenazas probables y el impacto que podría causar.

La realización del proceso por parte del Ingeniero Giovanny Sayas le da criterio para emitir su opinión y experiencia como usuario del sistema EBASF 1.0 (presentada en la sección siguiente).

7.4. DESCRIPCIÓN DE RESULTADOS DE LA PRUEBA

Realizada la prueba del modelo EBASF a través de la herramienta software que lleva su nombre, el consultor, Ing. Giovanny Sayas Acevedo, emite un documento donde resume su experiencia y opiniones al respecto, como resultado del procedimiento (véase en la siguiente página).

ESCENARIO DE PRUEBA: AKENDOS S.A.S

Tipo de Organización: Servicios	Usuario: Giovanny Sayas Acevedo	Fecha: 17 / 04 / 2012	
¿Tiene alguna experiencia en el manejo de Esquemas de seguridad informática?		SI: X	NO:
Mientras manejaba el software, las funciones le parecieron:	Muy Difíciles		
	Manejables		X
	Fáciles de usar		
¿Cree que el sistema es consistente? Hace lo que debe hacer?		X	
Mientras trabajaba en el sistema, ¿tuvo dificultades para navegar en éste?			X
En relación al contenido y documentación manejada en la herramienta, considera que el software tiene componentes educativos?		X	
¿Comprendió las temáticas incluidas en el desarrollo del modelo EBASF?		X	
¿El objetivo de la herramienta le fue claro?		X	
¿Estaría dispuesto a utilizar la herramienta para realizar el proceso completo de creación de políticas físicas en el centro de cómputo?		X	
¿Cree que un software de este tipo es una buena herramienta de apoyo en el proceso de creación de políticas?		X	
¿Qué opinión le merece el esquema básico de seguridad física propuesto?	Bueno		X
	Malo		
	Regular		
	Excelente		

Sugerencias:
la presentación de la documentación podría ser más dinámica.

7.4.1. DATOS RELEVANTES ENCONTRADOS Y OBSERVACIONES

El Consultor asignado por la empresa de desarrollo de software Akendos S.A.S (escenario de prueba) realizó las siguientes observaciones de mejora de la herramienta software, así como datos relevantes hallados.

- Se debe aclarar a las empresas interesadas en la implantación del modelo EBASF, (usando la herramienta software) la importancia de que el personal asignado cuente con los conocimientos mínimos requeridos.
- El manejo de las Dimensiones de Valoración en el desarrollo de la metodología de Análisis de Riesgos MAGERIT 2.0 es delicado, por lo tanto, se debe realizar un estudio previo, en el tiempo necesario, para comprender los diversos valores que se pueden asignar y con qué criterios.
- La aplicación de EBASF es importante para la toma de decisiones respecto a la implantación de políticas de seguridad en la empresa, debido a que permite determinar las amenazas más probables y su impacto en caso de materializarse.
- En una versión más avanzada de la aplicación se sugiere añadir un módulo que permita realizar un análisis de riesgos cuantitativo en la empresa, para conocer a nivel financiero cuánto se vería afectada.

En el estudio de casos prácticos de la metodología MAGERIT 2.0 realizados para corroborar resultados de la prueba relacionada anteriormente, con asesoría del Ingeniero en Informática Javier Cao Avellaneda, Consultor en seguridad de la Información, CISA y Auditor ISO 27001, se encontró que existe una herramienta denominada UPilar financiada por el Centro Criptológico Nacional (CCN) para la realización de este procedimiento; sin embargo, la herramienta tiene derechos reservados, además, fue diseñada a la medida por los interesados (Avellaneda, 2012). En este sentido, el Ingeniero sostiene que la herramienta EBASF es una buena propuesta dado que incluye el análisis de riesgos como parte del proceso de creación de las políticas de seguridad física, lo que según sus afirmaciones, se debe hacer para implementar medidas pertinentes.

7.5. RESULTADOS

En relación a los objetivos del proyecto, los resultados obtenidos con la ejecución del mismo son los siguientes:

La construcción de un completo referente teórico, que engloba desde seguridad informática hasta los estándares a ser estudiados, como parte del estado del arte y marco de requerimientos de la herramienta a desarrollar. Contacto y comunicación virtual con el Dr. Alvaro G. Vieites de España, (Caixanova, EOSA y SIMCe Consultores), Dr. Jeimy J. Cano (Universidad de los Andes), asesores en el proceso de investigación. Se aplicaron y diseñaron formatos de técnicas de recolección de información (TRI): Análisis de Contenido, Observación no estructurada y Encuesta (Sondeo); el análisis de los resultados delimitó el proyecto hacia seguridad física, por haber sido seccionado en seguridad física y seguridad lógica. Dado que las estadísticas muestran pérdidas financieras incalculables a raíz de incidentes que involucran fallas físicas, y errores humanos. Los incidentes alcanzan costos estimados de más de USD$3,000, 00 (Foundation, 2010).

Delimitado el proyecto, como parte inicial del diseño del esquema o modelo básico de seguridad informática, se realizó la selección de estándares internacionales de seguridad de la información más aplicados, se identificaron aspectos comunes que los caracterizan y permiten describir sus fines y forma de trabajar. Éstos se listaron y posteriormente se adecuaron dentro de una matriz que permitió evaluarlos equitativamente, en la medida en que se analizó como se comportaba la norma en un mismo sentido (sección 5.3). De esta forma se conocieron ventajas y desventajas.

El desarrollo de la sección de *análisis y fundamentos*, corresponde a la descripción de las estrategias técnicas y teóricas estudiadas, analizadas y aplicadas en la construcción del Esquema de Seguridad. La teoría de la dualidad constituyó el fundamento para la definición de la metodología a aplicar en la selección de características y elementos componentes del modelo. En efecto, a partir de la disciplina dual, se proyecta un estudio de la realidad del mercado, enfocado a lo que se está presentando en cuanto a inseguridad informática en las empresas, es decir, en lugar de preguntar a las empresas cómo responden los estándares a sus requerimientos, se evalúa cuáles son los requerimientos de las empresas a nivel de

seguridad física, y a partir de allí el grupo de trabajo determinó si los estándares respondían a éstos, cómo y mediante qué elementos lo hacían, para extraer, finalmente, características acordes a lo sucedido actualmente y lo que posiblemente ocurrirá con base en ello.

Sobre la base de las consideraciones anteriores, se realizó la investigación, extracción, clasificación y depuración de los datos de reportes mundiales sobre los incidentes de seguridad física realizados por la Open Security Foundation mediante la base de datos DatalossDB[14]. Igualmente, se revisaron estadísticas y tendencias en Colombia y Latinoamérica. Como resultado de estos razonamientos se establecieron los *criterios de evaluación* de los estándares, asignando una valoración, de acuerdo a la escala planteada; así de seleccionaron y adaptaron características y elementos de COBIT, RFC2196, ISO 27001, ISO 17799 y TCSEC, que permitieron estructurar el esquema de solución propuesto en la investigación (sección 5.6).

Se diseñó la arquitectura del software que corresponde a la implementación del esquema EBASF (Esquema básico de Seguridad Física), a través de modelos en herramientas I-CASE, que representan las diferentes funcionalidades de la herramienta, siguiendo el modelo 4+1 vistas, y el patrón de diseño software MVC. El consolidado final de la investigación, es el presente documento (destacando la sección 5.6 de estructuración del modelo), donde se plasman los resultados teóricos y prácticos.

La participación de la ponencia "**Políticas de Seguridad Informática: herramienta clave para la continuidad de la organización**" en el I Congreso Internacional de Investigación y Administración, fue el mecanismo para divulgar aspectos representativos de la investigación y mostrar resultados preliminares del proyecto (Ver Anexo 7.4.1).

Se presentan resultados experimentales del proyecto, mediante aplicación del esquema a través del uso de la herramienta software por parte del consultor asignado de la empresa Akendos S.A.S, como escenario seleccionado para ello (generalidades de la prueba y análisis de resultados en la sección anterior.

[14] Para conocer mayor información sobre la base de datos, ingrese a: http://datalossdb.org/.

8. CONCLUSIONES Y RECOMENDACIONES

8.1. CONCLUSIONES

La información constituye uno de los activos más valiosos para las empresas. Dada su importancia en todos los procesos en la organización será necesario mantenerla segura, para que se encuentre donde se necesita, en el momento que se necesita y en las condiciones que es requerida. Actualmente, es el motor de la era digital en que se mueve el mundo, por lo tanto, se encuentra expuesta a muchos riesgos a lo largo de todo su manejo, desde que es generada, hasta que es almacenada.

Han sido numerosos los hechos que incluyen pérdidas de información ocasionadas por la falta de seguridad. De allí el origen de numerosos modelos, metodologías, estándares o normas elaboradas con el fin de dar pautas en el establecimiento de Políticas de Seguridad Informática (PSI); sin embargo, la aplicación de éstos, ha sido una tarea difícilmente asumida por las empresas, dada su complejidad. El presente proyecto estuvo enfocado a verificar esta última afirmación, que constituyó la pregunta de investigación, y en consecuencia la formulación del problema a resolver.

Con referencia a lo anterior, en revisiones de investigaciones previas, el grupo de trabajo halló el ESTUDIO DE UNA ESTRATEGIA PARA LA IMPLANTACIÓN DE LOS SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN del autor (Barcell, 2003), quien precisa en su informe: *"Muchas organizaciones no abordan de modo serio una política de seguridad "formal" (según norma) por la complejidad de la misma. Las metodologías y normas existentes relacionadas con los SGSI no aclaran sus ámbitos de aplicación, resultando una amalgama de normas de compleja aplicación. Esto reduce su posible implantación a las grandes corporaciones".* Estudios como éste evidencian la necesidad de implementar herramientas de apoyo para el establecimiento de políticas y esquemas de seguridad informática en las empresas; principalmente a nivel nacional.

En este sentido, la estructuración del esquema de referencia básico propuesto como solución en el presente proyecto, estuvo marcada por investigaciones amplias que además de confirmar la complejidad asociada a la selección y aplicación de estándares, permitieron responder a los objetivos planteados, a través de diferentes métodos, como la dualidad de la seguridad informática, técnicas formales de recolección de información, el análisis estadístico de informes, y la determinación de criterios de evaluación de estándares para la consolidación del Esquema.

Respecto al enfoque dual, es pertinente concluir que, ha sido factor clave para el desarrollo de muchos conceptos que hoy en día son esenciales para el avance no sólo de la tecnología sino de la seguridad informática, porque se presenta como una manera complementaria de comprender los elementos, relaciones y efectos de la seguridad informática en el contexto de una realidad cambiante y dinámica. Convirtiéndose en una estrategia que permite trascender a la par de los posibles avances que puedan generar amenazas a nuestros sistemas. Por lo tanto, el modelo EBASF, es una herramienta con fundamentos sólidos, que ofrece pautas de creación de políticas de seguridad física soportadas en los requerimientos del mercado y elementos de estándares internacionales, proyectados en las etapas, orden de trabajo del modelo, alineación estratégica aplicada, análisis de riesgos, pautas de seguridad física, sugerencias específicas, documentación metodológica, revisión frecuente, manejo de correcciones y trabajo en Ciclo.

Cabe destacar que la definición de los estándares de seguridad estudiados es muy general, es decir, no es específica hacia la creación de PSI, lo que limitó en cierto momento la determinación de criterios de comparación y evaluación de éstos, para construir un esquema que respondiera a los requerimientos de seguridad física detectados en estudios preliminares.

Por otro lado, los estudios dejan entrever que una política de seguridad bien implantada es aquella que refleja los objetivos de negocio de la empresa. Y para lograr el éxito en la implantación, es necesario tener el apoyo y crear conciencia en la alta dirección de la empresa. Además, un esquema de seguridad puede comprender una gran variedad de ámbitos dentro de la empresa y éstos se seleccionan en base a la importancia de cada uno

en los negocios de la misma. Así mismo, puede atender diferentes intereses de seguridad (confidencialidad, integridad, disponibilidad, autenticidad) que serán de mayor interés en una organización que en otra.

El trabajo desarrollado fue una experiencia enriquecedora no sólo a nivel profesional sino personal; los miembros del equipo se integraron para realizar tareas de recolección de información, análisis de datos, construcción de conceptos, comprensión y aplicación de teorías, entre otros, que permitieron el intercambio de conocimientos, destrezas y valores humanos, además del fortalecimiento del nivel intelectual.

El producto final constituye un modelo conceptual que describe procesos y pautas a desarrollar en la creación de políticas de seguridad físicas. Acompañado del sistema software EBASF como implementación del mismo y herramienta de facilitación y consolidación de metas.

Para concluir, *"Una política de seguridad se convierte en el primer paso para lograr que la seguridad sea un esfuerzo común, habilitando el desarrollo de una arquitectura de seguridad de la información."*

8.2. RECOMENDACIONES

Tomando como precedente los resultados planteados, se recomienda seguir trabajando en la consolidación del Macro proyecto. Lo que implica completar la parte de apoyo en la creación de políticas de Seguridad Lógica, dado que esta investigación se delimitó a la Seguridad Física. Las bases teóricas adelantadas en el proyecto, pueden agilizar su implementación.

Igualmente, se recomienda el estudio y materialización software del estándar internacional ISO 27001, para empresas que apliquen el esquema básico y requieran posteriormente certificación.

La utilización del modelo EBASF y la aplicación, requiere de tiempo y dedicación. Por lo que se sugiere asignar una persona que cumpla el rol de Consultor o Usuario encargado de las tareas, para lograr una implementación adecuada.

El software contiene documentación extendida, que no debe ser pasada por alto al momento de realizar el proceso de creación de políticas, porque esto puede ocasionar errores.

ANEXO 7.4.1

El siguiente documento corresponde al certificado emitido por la entidad organizadora del evento internacional, donde se realizó la presentación de la ponencia "Políticas de Seguridad Informática: herramienta clave para la continuidad de la organización" como mecanismo para divulgar aspectos representativos de la investigación.

UNIVERSIDAD SIMÓN BOLÍVAR

CENTRO DE EDUCACIÓN CONTINUADA
UNIVERSIDAD SIMÓN BOLÍVAR

Certifican que:

RONALD NÚÑEZ

Participo como CONFERENCISTA

1er. CONGRESO INTERNACIONAL DE INVESTIGACIÓN EN ADMINISTRACIÓN

"La Competitividad y la Innovación en la Empresa de Hoy"

Programa de Administración de Empresas

Dado en Barranquilla a los 28 días del mes de octubre de 2011

Lourdes Truyol de Rica
LOURDES TRUYOL
Centro de Educación Continuada

Ana Blanco Ariza
ANA BLANCO ARIZA
Programa de Administración de Empresas

REFERENCIAS

Albanés, A. J. (s.f.). Tema 1. Introducción a la Ingeniería del Software(ISG1-ITIG). En A. J. Albanés. España: Universidad de Sevilla.

Amaya, M. J. (23 de Septiembre de 2004). Seguridad informática. *Seguridad informática: Estamos seguros?*

Asociación Colombiana de Ingenieros de Sistemas. (2011). *ACIS*. Recuperado el 2 de febrero de 2011, de ACIS: www.acis.org.co

Barcell, M. F. (2003). *ESTUDIO DE UNA ESTRATEGIA PARA LA IMPLANTACIÓN DE LOS SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN.* España: Universidad de Cádiz.

Borghello, C. (2008). *Segu-Info Seguridad de la Información, 11 años educando en seguridad.* Recuperado el 20 de 09 de 2011, de Seguridad Física: http://www.segu-info.com.ar/fisica/seguridadfisica.htm

Borghello, C. F. (14 de 10 de 2010). *Segu-Info, Seguridad de la Información*. Recuperado el 14 de enero de 2011, de Certificación CISSP: http://www.segu-info.com.ar/articulos/54-certificacion-cissp.htm

Borghello, C. F. (Septiembre de 2010). *Seguridad Informática, sus implicancias e implementación.* Universidad Tecnológica Nacional.

Calderón, G. S. (2010). Seguridad informática en el Estado. *Eltiempo.com, 1*.

Cano, J. J. (2008). *Seguridad Informática en Colombia, tendencias 2008.* ACIS.

Cano, J. J. (2009). *IX Jornada de Seguridad Informática, Monitoreo y Evolución de la Inseguridad Informática.* ACIS.

Cano, J. J. (2010). *Aprendiendo de la Inseguridad Informática*. Obtenido de Asociación Colombiana de Ingenieros de Sistemas, ACIS: http://www.acis.org.co/index.php?id=457

Cano, J. J. (2010). *Inseguridad Informática: Un concepto dual en Seguridad Informática.* Barranquilla: Universidad de los Andes.

Cano, J. J., & D, E. A. (2010). *II Encuesta Latinoamericana de Seguridad de la Información, ACIS 2010.* Bogotá: JCM10.

CEAS EDUCACION. (2010). Recuperado el 21 de Agosto de 2010, de MASTER EN SEGURIDAD INFORMATICA: http://www.cisedu.org/cursos/msi.html

CERINI, M. D. (Octubre de 2002). PLAN DE SEGURIDAD. *PLAN DE SEGURIDAD*. Córdoba, Colombia, Colombia: UNIVERSIDAD CATÓLICA DE CÓRDOBA.

ChannelPlanet Inc. (2006). *ChannelPlanet Investigación, medios y eventos en tecnología de información*. (ChannelPlanet) Recuperado el 15 de febrero de 2011, de El modelo COBIT para auditoría y control de sistemas de información: http://www.channelplanet.com/index.php?idcategoria=13932

COL-CSIRT . (s.f.). *COL-CSIRT* . Recuperado el 10 de febrero de 2011, de CFE – Certified Fraud Examiner: http://gemini.udistrital.edu.co/comunidad/grupos/arquisoft/colcsirt/?q=node/2

Colombia, U. N. (2003). Guia para la elaboraciòn de politicas de seguridad. Bogota, Colombia : Tipton & krausen .

Crespo, F. L. (2005). *MAGERIT Versión 2*. Madrid: Ministerio de Administraciones Públicas - NIPO.

DAEDALUS. (s.f.). *Qué es el Conocimiento.* Obtenido de DAEDALUS - Data, Decisions and Language S.A.: http://www.daedalus.es/inteligencia-de-negocio/gestion-del-conocimiento/que-es-el-conocimiento/

Definicion.com . (s.f.). *DEFINICIÓN*. Recuperado el 12 de Octubre de 2010, de DEFINICIÓN.

Departamento Administrativo de Ciencia, Tecnología e Innovación. (s.f.). *Colciencias*. Recuperado el 10 de 02 de 2011, de Colciencias: http://www.colciencias.gov.co/sobre_colciencias

Estándar Internacional ISO/IEC 27001. (15 de Octubre de 2005). *Tecnologías de la información, técnicas de seguridad, Sistemas de gestión de seguridad de la información*.

Fites, P. e., & Kratz, M. P. (1989). *Information Systems Security* . New York: Van Nostrand Reinhold.

Foundation, O. S. (2010). *DataLossDB Open Security Foundation.* Recuperado el 14 de 09 de 2011, de DataLossDB Database - 2011 yearly report: http://datalossdb.org/

Gerrero, E. L. (s.f.). Lámina de ajuste. *ISO 17799 Normas Internacionales para la Regulación de la seguridad de la Información* .

Howard, P. D. (2003). Guía para la elaboración de Políticas de Seguridad, Universidad Nacional de Colombia. Bogotá, Colombia, Colombia: Tipton and Krause.

Huerta, A. V. (2004). *El Sistema de Gestión de Políticas de Seguridad de la Información.* Valencia.

Institute, I. G. (2005). *CobiT 4.0.* Estados Unidos: GLANSER SERVICES, S.C.

Instituto Financiero para el Desarrollo del Valle del Cauca. (s.f.). *Infivalle*. Recuperado el 10 de 02 de 2011, de Infivalle: http://www.infivalle.gov.co/index.php?module=htmlpages&func=display&pid=1

ISACA. (s.f.). *ISACA Trust in, and value from, information systems*. (ISACA) Recuperado el 20 de febrero de 2011, de Certified Information Systems Auditor (CISA) : http://www.isaca.org/Certification/CISA-Certified-Information-Systems-Auditor/Pages/default.aspx

ISACA. (s.f.). *ISACA, Trust in, and value from, information systems*. Recuperado el 10 de febrero de 2011, de What is CISM: http://www.isaca.org/Certification/CISM-Certified-Information-Security-Manager/What-is-CISM/Pages/default.aspx

iSoluciones. (19 de julio de 2007). *Seguridad informática en PYMEs. Un marco actual*. Recuperado el 2 de octubre de 2010, de iSoluciones, Blog de experiencias en auditoría y seguridad informática.: http://isoluciones.blogspot.com/2007/07/seguridad-informtica-en-pymes-un-marco.html

Jiménez R., M. (s.f.). Diseño de Información. En *El ensayo fotográfico en el diseño de información. El uso de la fotografía en la investigación exploratoria de un fenómeno social.* Universidad de las Américas Puebla.

Junco, A. R. (2009). *Encuesta nacional Seguridad Informática en Colombia: Tendencias 2010.* ACIS.

Ministerio de Administraciones Públicas, S. G. (2004). *Organisation for Economic Co-operation and Development (OECD).* España.

Moreno, N., & Rodríguez, F. (s.f.). *La Gestión de la Información como base de la Gestión del Conocimiento y del Aprendizaje Organizacional en las Universidades.* Obtenido de http://docs.google.com/viewer?a=v&q=cache:tW_E-Aqi2sUJ:www.dict.uh.cu/Revistas/Educ_Sup/022002/Art030202.pdf+gestion+de+la+informacion&hl=es&gl=co&pid=bl&srcid=ADGEESjULMRHb5n8FqDcP2VFa3HgmvJ4GPQ8T98mRT9XCw069UnxqFZbLzuQ-sLrq0V9hWP4-U1Fjj-S9zUfX19-PXsR59Y

Murillo, S. R. (Mayo de 2010). ASIS: Diseño y Aplicación de un Sistema Integral de Seguridad Informática para UDLA. *Capítulo 1: Conceptos básicos de Seguridad Informática*. Puebla, México, México.

New Horizons Barcelona. (s.f.). *New Horizons Computer Learning Center, Líder el Informática*. (New Horizons) Recuperado el 14 de febrero de 2011, de Certificación ITIL, (IT Infrastructure Library) : http://www.nhbarcelona.com/certificaciones/itil.htm

Paz, D. C. (s.f.). CONCEPTOS Y TÉCNICAS DE RECOLECCIÓN DE DATOS EN LA INVESTIGACIÓN JURÍDICO SOCIAL. Londres.

Pfleeger, C. P. (2003). *Security in computing.* Jane Bonnel.

Rodríguez R., J., de Miguel, T., & Monroy R., M. (s.f.). *Arquitectura Web 2.0 para la Federación de Servicios en Comunidades Virtuales de Aprendizaje.*

Saavedra, I. (30 de junio de 2009). *Seguridad informática para pymes: ¿Gasto o inversión?* Recuperado el 28 de Octubre de 2010, de Baquia Knowledge Center: http://www.baquia.com/articulos/innovacion/noticia/15032/seguridad-informatica-para-pymes-gasto-o-inversion

Sandoval, C. A. (01 de junio de 2010). *Sistema Integral de Gestion Registral.* Recuperado el 2 de Septiembre de 2010, de SIGER: http://www.firmadigital.gob.mx/

Scribd. (2010). Recuperado el 20 de 2 de 2011, de Qué son las herramientas CASE?: http://es.scribd.com/doc/3062020/Capitulo-I-HERRAMIENTAS-CASE

Universia Noticias Colombia. (22 de enero de 2009). *Universia.* Recuperado el 2 de febrero de 2011, de Universia, red de Universidades, red de Oportunidades: http://noticias.universia.net.co/publicaciones/noticia/2009/01/22/239003/seguridad-informatica-es-realidad-colombia-gracias-proyecto-investigacion-icesi.html

versvs . (27 de 11 de 2007). *versvs, más allá de las transformaciones de Fourier*. Recuperado el 10 de febrero de 2011, de versvs : http://www.versvs.net/anotacion/que-es-un-erp-enterprise-resource-planning-linux

Vieites, A. G. (2008). *CONSIDERACIONES SOBRE LA DEFINICION DE UN PLAN DE RESPUESTA A INCIDENTES DE SEGURIDAD.* Caixanova: Escuela de Negocios Caixanova.

Vieites, A. G. (2009). *DIRECTRICES PARA LA DEFINICION E IMPLANTACION DE POLITICAS DE SEGURIDAD.* Caixanova: Escuela de Negocios Caixanova.

Virusprot. (2010). Recuperado el 20 de Agosto de 2010, de Virusprot: www.virusprot.com

Wikipedia. (28 de septiembre de 2010). Recuperado el 10 de septiembre de 2010, de Wikipedia: http://es.wikipedia.org/wiki/Seguridad_inform%C3%A1tica

Wikipedia. (20 de mayo de 2011). *Wikipedia, La enciclopedia libre*. Recuperado el 30 de enero de 2011, de Wikipedia: http://es.wikipedia.org/wiki/Proceso_Unificado_de_Rational