Universidad de Costa Rica
Sistema de Estudios de Posgrado

Auditoría de los controles de seguridad para Consultores Asociados S.A.

Trabajo Final de Graduación aceptado por la Comisión del Programa de Posgrado en Administración y Dirección de Empresas, de la Universidad de Costa Rica, como requisito parcial para optar al grado de Magíster en Auditoría de Tecnologías de la Información.

Carlos Andrés Casas Cruz
A56962

Ciudad Universitaria "Rodrigo Facio", Costa Rica
Año 2007

1 Dedicatoria

A los profesionales de la auditoría de tecnología y a las personas que lean este trabajo.

2 Agradecimientos

A Dios por la iluminación en el camino de la maestría. A mi esposa Lorna, a Daniel mi hijo y a mis padres Amanda y Carlos, por el apoyo y comprensión durante este proceso.

3 Hoja de Aprobación

Este Trabajo Final de Graduación fue aceptado por la Comisión del Programa de Posgrado en Administración y Dirección de Empresas, de la Universidad de Costa Rica, como requisito parcial para optar al grado de Magíster en Auditoría de Tecnologías de la Información.

_____

Doctor, Aníbal Barquero Chacón,

Director Programa de Maestría

_____

Master Sergio Espinoza Guido,

Profesor Coordinador

_____

Master, Xiomar Delgado Rojas, CISA,

Profesor Guía

_____

Master Franklin Noguera Flores

Supervisor Laboral

_____

Carlos Andrés Casas Cruz

Estudiante

4 Índice del contenido

5 Índice de Gráficos

6 Índice de Tablas

7 Índice de Anexos Complementarios

8 Índice de Siglas y Abreviaturas

Committee of Sponsoring Organizations of the Treadway Commission	COSO
Enterprise Risk Management	ERM
National Institute of Standards and Technology	NIST
Universidad de Costa Rica	UCR
Tecnologías de Información	TI
Common Vulnerabilities and Exposures	CVE
Virtual Private Network	VPN
Normas Internacionales de Auditoría	NIA
Local Area Network	LAN
Wide Area Network	WAN
Uninterruptible Power Supply	UPS
International Organization for Standardization	ISO

9 Resumen

La auditoría informática de seguridad es la revisión y la evaluación de los controles y procedimientos de la organización tendientes a brindar integridad, confidencialidad y disponibilidad al procesamiento de la información, a fin de que por medio del señalamiento de cursos alternativos se logre una utilización más eficiente y segura de la información que servirá para una adecuada toma de decisiones.

El objetivo general del trabajo es identificar si los controles de seguridad implementados en la firma Consultores y Asociados S.A., soportan de manera razonable el procesamiento de la información y preservan su integridad, confidencialidad y disponibilidad.

La organización investigada se dedica a Brindar servicios de Consultoría construcción y avalúos.

En las secciones posteriores se detallan las recomendaciones basadas en normas aceptadas por la industria (ISO 17799) y cubre los aspectos principales de la seguridad de la información recomendada para la empresa seleccionada en este trabajo. Estas recomendaciones van en función de las siguientes áreas de seguridad informática que formaron parte de la evaluación conducida:

- → Seguridad organizacional.
- → Políticas de seguridad.
- → Arquitectura de seguridad en redes.
- → Prácticas de monitoreo para la seguridad.
- → Procesos de seguridad en los recursos humanos.
- → Planes de contingencia.
- → Programas de capacitación.

- → Vulnerabilidades técnicas en oficinas centrales, oficinas regionales y asociaciones.
- → Seguridad Física, controles para la concientización y destrucción de documentación sensitiva.

Durante el transcurso de la evaluación mencionada, se identificaron punto de mejora, donde cada una de ellas fue ampliamente valorada y discutida en el documento de Recomendaciones discutido con la gerencia de TI.

10 Introducción

El presente trabajo pretende generar una guía de auditoría que pueda ser aplicada a cualquier proceso de tecnología y demostrar por medio de una evaluación de controles de seguridad su aplicación.

10.1 Antecedentes del problema

10.1.1 El riesgo

Todas las organizaciones están sujetas a enfrentar algún tipo de riesgo día con día. La administración de riesgo es una tarea que requiere disciplina para tratar con los riesgos no especulativos[1], en la cual existe la posibilidad de ganar o perder, como por ejemplo, las apuestas o los juegos de azar. En cambio el riesgo puro es el que se da en la empresa y existe la posibilidad de perder o no perder, pero jamás ganar. Estos peligros por lo general están sujetos a una administración de riesgo empresarial con el objetivo de reducir el impacto y el deterioro de valor que un evento desfavorable le pueda ocasionar a los activos de la empresa.

Un programa de administración de riesgo empresarial, por lo general tiene 4 puntos a considerar en el tratamiento de los mismos:

1. Eliminar el riesgo.
2. Reducir el impacto de los riesgos que no se puedan eliminar a un nivel razonable.
3. Convivir con el riesgo.
4. Transferir el riesgo.

Es importante medir el riesgo en términos económicos, para identificar si las estrategias de administración son de beneficio para la organización basado en un análisis económico que la organización podría costear para implementar un

[1] Víctor, Belmar, *Prevención de riesgos - Implantación de un sistema efectivo de control del riesgo operacional en la empresa,* http://www.monografias.com/trabajos13/progper/progper.shtml

control en particular. Es conveniente que para todo control que la organización vaya a implementar, exista un análisis económico de su costo beneficio. Las empresas deberían poseer un criterio a aplicar para identificar si se acepta el riesgo y no se implementan controles, por ejemplo, si el impacto económico es menor que el precio de controlarlo, será más efectivo no controlarlo.

La administración de riesgos no debe ser una actividad de alto nivel o estratégica. En los últimos 5 años se han creado o modificado nuevas regulaciones y estándares que solicitan evaluarlo, con el objetivo que la empresa demuestre haber tomado acciones razonables para tratar los riesgos identificados, generando un balance entre el costo de administrar el riesgo y el beneficio adquirido.

Estás regulaciones o estándares que se reconocen con el nombre:

- Basilea 2.
- ISO 17799.
- Sarbanes Oxley.
- Normativa de tecnología de información para las entidades fiscalizadas por la superintendencia general de entidades financieras Costa Rica.

El proceso de evaluación de riesgo formal debe estar estructurado, pasando por las etapas de planeación, recolección de información, análisis de la información y generación de resultados. Cuando se refiere a un proceso formal no se pretende obligar el uso de una aplicación o software para la realización de la evaluación; sin embargo, éste sería de útil apoyo durante el proceso. Las técnicas utilizadas para evaluar el riesgo deben ser lo suficientemente complejas para satisfacer las necesidades de la organización.

En las empresas por lo general la administración designa a un encargado de guiar o realizar el proceso de evaluación de riesgos; sin embargo, existen dos factores o claves a considerar, el primero es que los estándares y las normativas exigen revisiones periódicas de los riesgos y controles para identificar nuevas

vulnerabilidades en el ambiente y evaluación del impacto que éstas puedan tener o simplemente ratificación de que los controles implementados permanecen válidos y son efectivos. Estas revisiones periódicas son fundamentales dentro de los procesos de evaluación de riesgo o estrategias de administración de los mismos.

La segunda es poseer personal con la experiencia y las competencias necesarias. Es esencial que la evaluación de riesgos sea realizada por personal calificado, pues de esta forma será posible obtener un resultado más acertado.

Las organizaciones que han identificado que la administración de riesgos es una tarea esencial para el negocio, seguro ya poseen personal capacitado y especializado que les permite llevar a cabo las evaluaciones de riesgo.

10.1.2 La Contabilidad

En cualquier punto de la tierra y momento de la historia, la sociedad en general, han sentido y siente la necesidad de conocer con qué recursos cuentan y cómo ejercer un control sobre los mismos, de forma que logren aumentar sus posibilidades de acumulación o, al menos, no caer en una situación económicamente negativa.

En la era de las grandes civilizaciones como Mesopotamia, Egipto, Grecia o Roma hasta las doctrinas actuales de contabilidad, se ha hecho hincapié en conocer los ingresos y los gastos por medio de la partida doble como se conoce actualmente, donde su postulado[2] principal es:

> *"No hay deudor sin acreedor, ni acreedor sin deudor". Esto significa que, considerando la totalidad de los elementos patrimoniales de la empresa, si un elemento disminuye es porque otro aumenta, o, lo que es lo mismo, si se produce una entrada en un elemento es porque hay una salida*

[2] Definición de Partida Doble, Diccionario Wikipedia, http://es.wikipedia.org/wiki/Partida_doble

de otro elemento y, por tanto, hacer un cargo en una cuenta (o cuentas) supone siempre tener que hacer un abono en otra (u otras).

En el inicio del comercio, las empresas o comerciantes presentaron el interés de registrar cada movimiento que se realizaba y con la llegada de la revolución industrial, el conocer sobre los activos de la empresa y el beneficio recibido, tomó mayor importancia; sin embargo, el cambio que dio un giro radical al tratamiento de la información se presenta en el década de 1960 con las primeras computadoras o mainframes, que fueron utilizadas para el procesamiento de información contable y otras implementaciones para el control de la nómina, hicieron que las empresas dedicaran parte de su presupuesto en tecnología.
Desde entonces la contabilidad y la tecnología fueron madurando hasta el punto actual donde casi todas las empresas poseen un software contable utilizado para registrar, clasificar y resumir las transacciones operativas y financieras del negocio con el fin de interpretar sus resultados.

10.1.3 La Auditoría

Según la definición del diccionario de la Real Academia de la Lengua Española, un auditor es una "*persona nombrada por el juez entre las elegidas por el obispo o entre los jueces del tribunal colegial, cuya misión consiste en recoger las pruebas y entregárselas al juez, si surge alguna duda en el ejercicio de su ministerio"*[3].

La palabra auditoría es la ejecución de labores que realiza el auditor. Por su definición, se denota que un auditor es una persona de alta confianza encargada de validar la veracidad de un acontecimiento o serie de acontecimientos. Cuando se le pregunta a una persona que entiende por auditoría, las respuestas

[3] Diccionario de la Lengua Española, Ed. Electrónica en CD-Rom, versión 1.0.

por lo general van enfocadas a definir una persona que vigila o controla la realización de acciones o procesos.

En las empresas el auditor se encarga de validar riesgos y los controles implementados para mitigar dichos riegos en función de la consecución de los objetivos empresariales. Es normal ver empresas donde se confunde la función del auditor y se le asignan tareas como la definición y establecimiento de los controles cuando, en realidad, esta función corresponde a la administración, pues en caso de que el auditor se preste para la realización de esta labor, estaría actuando como juez y parte, al cumplir la tarea de diseñar los controles y luego evaluar si son suficientes y adecuados, restándole objetividad y credibilidad a su trabajo.

Una vez que se ha identificado lo que no debe ser un auditor, el Instituto de Auditores Internos define a la auditoría como[4]:

> *"Una actividad independiente y objetiva de aseguramiento y consulta, concebida para agregar valor y mejorar las operaciones de una organización. Ayuda a una organización a cumplir sus objetivos aportando un enfoque sistemático y disciplinado para evaluar y mejorar la eficacia de los procesos de gestión de riesgos, control y gobierno."*

[4] The Institute of Internal Auditor, *Definición de la auditoría interna*, http://www.theiia.org/guidance/standards-and-practices/professional-practices-framework/definition-of-internal-auditing/?search=audit%20definition

10.2 Justificación

Es muy importante que las empresas justiprecien toda la inversión de recursos que consume un departamento de tecnología y las ventajas que se obtienen cuando se aplican controles que permiten hacer un uso racional de la inversión, maximizando la ganancia y el bienestar de los empleados. Es así como la auditoría informática, genera valor a la entidad por medio de la identificación de riesgos y evaluación de los controles que mitigan dichos riesgos.

Como lo declara la Norma Internacional de Auditoría (NIA) 620 Uso del Trabajo de un Experto, la NIA 315 Entendimiento de la Entidad y su Entorno y 330 Procedimientos del Auditor en Respuesta a los Riesgos Evaluados, que proporciona la orientación necesaria para cumplir con los principios básicos de auditoría cuando ésta es llevada a cabo en un ambiente computacional. A los fines de esta norma, existe un ambiente de sistemas de información computarizada cuando un computador de cualquier tipo o tamaño es utilizado por la entidad en el procesamiento de información financiera de importancia para la auditoría, ya sea que el computador es operado por la entidad o por un tercero. Enfatiza que el auditor debería conocer en forma suficiente el hardware y los sistemas de procesamiento para planificar el trabajo y comprender en qué manera afectan al estudio y a la evaluación del control interno y la aplicación de los procedimientos de auditoría que incluye técnicas asistidas por computador.

Este proyecto hará que se tengan nuevos discernimientos de la realidad de la auditoría informática y promoverá a que se amplíe y abarque en forma integral las áreas que conforman un departamento de tecnología. Además, la entidad evaluada y otras empresas contarán con un estudio e investigación que les ayudará a implementar una auditoría informática.

10.3 Planteamiento del problema

La información electrónica producida por las empresas durante su gestión diaria, genera un valor intangible para el negocio y dependencia de ella. Para la administración, es factor importante resguardar dicho recurso y preservar su integridad, confidencialidad y disponibilidad; por lo tanto, se considera como agente de importancia la seguridad que se le aplique a este recurso y el correcto uso y maximización de beneficios que puedan generar las tecnologías y métodos de seguridad adquiridos e implementados.

En este punto, el rol de auditor es evaluar los controles internos implementados en el ambiente computacional, con el fin de validar si los procedimientos y prácticas de administración utilizados están enfocados en mantener la integridad, confidencialidad y disponibilidad de la información y a su vez identificar el correcto uso y aplicación de la tecnología en este proceso de resguardo.

10.4 Alcance y límites de la investigación

El proyecto abarcará la validación de los controles de seguridad implementados en el ambiente de procesamiento computacional de la firma Consultores y Asociados S.A. Dicha evaluación incluye:

- ✓ Recopilación de conceptos adquiridos durante el programa de Maestría, para formular la metodología de auditoría a aplicar.
- ✓ Comprensión del ambiente computacional.
- ✓ Identificación de riesgos.
- ✓ Identificación de controles clave a evaluar.
- ✓ Preparación de guías de auditoría.
- ✓ Ejecución de pruebas.
- ✓ Análisis de resultados.

- ✓ Preparación de informe final.

Por efectos de confidencialidad de la información recibida, no es factible divulgar el nombre de la Entidad evaluada.
Durante el desarrollo del proyecto, se utilizará la información recibida en el programa de maestría con el objetivo de demostrar la utilidad de este programa de estudio, el principal uso será en la definición de la metodología de auditoría.
Este proyecto no contempla el análisis de las funciones que proveen las herramientas de software a utilizar en la ejecución de pruebas.

10.5 Aportes

El presente proyecto representa dos aportes a manera de objetivo, el primero consiste en la aplicación de una metodología para la realización de auditorías informáticas que podrá ser aplicada en cualquier área de los controles generales. Esta metodología será la compilación de conocimientos y métodos vistos durante el programa de estudio, que como fruto final suministrará al auditor las guías de trabajo a aplicar. El segundo objetivo pretende generar valor a la Entidad por medio de la las recomendaciones a sugerir, producto de la evaluación de los controles generales.

11 Objetivos

11.1 General

Identificar si los controles de seguridad implementados en la Entidad, proveen integridad, confidencialidad y disponibilidad de manera razonable a la información que está maneja en sus sistemas de aplicación.

11.2 Específicos

1. Definir la metodología de trabajo para el proceso de evaluación de los controles generales del computador y a su vez que permita:

   a) Identificar las condiciones a evaluar.
   b) Definir el procedimiento para evaluar la condición.
   c) Ejecución de las pruebas definidas.
   d) Análisis de resultados.
   e) Conclusión y recomendación

2. Construir valor por medio de las recomendaciones emitidas en el informe final.

11.3 Contenido Capitulario

En el primer capítulo se realiza una descripción de la metodología de auditoría a aplicar durante la evaluación, las herramientas que la componen y como aplicar estas herramientas en un entorno empresarial real.

En el segundo capítulo se realiza la aplicación de la metodología descrita en el primer capitulo en un ambiente empresarial real y ejemplifica la aplicación de las herramientas descritas, finalizando con el informe de auditoría que procura generar valor a la organización.

En el tercer capítulo se concluye con los resultados de aplicar la metodología planteada, las lecciones aprendidas y consejos para futuras aplicaciones.

12 Capítulo 1: Metodología de Trabajo PEC

12.1 ¿Qué es Metodología PEC?

Según como lo define el diccionario de la Real Academia de la Lengua Española[5], metodología es:

> *"Conjunto de métodos que se siguen en una investigación científica o en una exposición doctrinal."*

Tomando como base la anterior definición, la Metodología PEC es la guía a utilizar para desarrollar un trabajo o proyecto en forma ordenada y eficaz, en este caso de auditoría informática que hace ineludible su aplicación. La metodología PEC, llamada así por las unidades de:

- → Planificación.
- → Evaluación del control.
- → Comunicación de resultaros.

brinda una guía detallada de los pasos que deberá aplicar el evaluador, desde la definición del objetivo de auditoría, pasando por el proceso de evaluación y finalizando en la opinión sobre el objetivo planteado. Este método podría compararse analógicamente con la necesidad que tiene un investigador de seguir el método científico para evitar generar conclusiones erróneas.
La simplicidad del modelo de 3 fases y correspondencia de los sub-procesos definidos en cada una de las fases, le brinda al evaluador las herramientas para asegurar concordancia entre el objetivo de auditoría y las recomendaciones identificadas. Esta metodología no obliga al evaluador a aplicar un marco de control específico, queda a su elección identificar qué marco de control se ajusta al ambiente evaluado.

[5] Diccionario de la Lengua Española, Ed. Electrónica en CD-Rom, versión 1.0.

La fase de planeación pretende definir un objetivo inicial de auditoría e introducir al evaluador en el entorno del negocio y su estructura de control interno, permitiéndole finalizar con una idea preliminar sobre el diseño de los controles relacionados, con el objetivo evaluado y proponiendo su plan de auditoría. Es importante indicar que al finalizar esta fase, el evaluador deberá identificar, según su criterio profesional, si el objetivo inicial de auditoría se mantiene vigente acorde a los riesgos identificados y el diseño de controles que posee la entidad, o es conveniente re-plantearlo, enfocándolo a los riesgos identificados y así generar más valor a la organización con el proceso de revisión.

Definido el objetivo final de auditoría y evaluado el diseño de los controles existentes, el evaluador deberá validar la implementación de los mismos y su eficacia a través del período cubierto en la revisión. Durante este proceso de evaluación se identificará qué controles no han sido implementados o no operan de manera eficiente y podrá emitir recomendaciones que serán discutidas con la administración y expresadas en el informe final de la auditoría. Una imagen gráfica del flujo del proceso de auditoría se presenta en el Gráfico 1.

Esta metodología es un compendio de los conocimientos adquiridos durante el programa de Maestría de Auditoría Informática de la Universidad de Costa Rica y hace uso de las herramientas desarrolladas durante el programa y los conceptos formados. Los créditos de cada fuente utilizada serán mencionados durante la descripción de cada una de las fases.

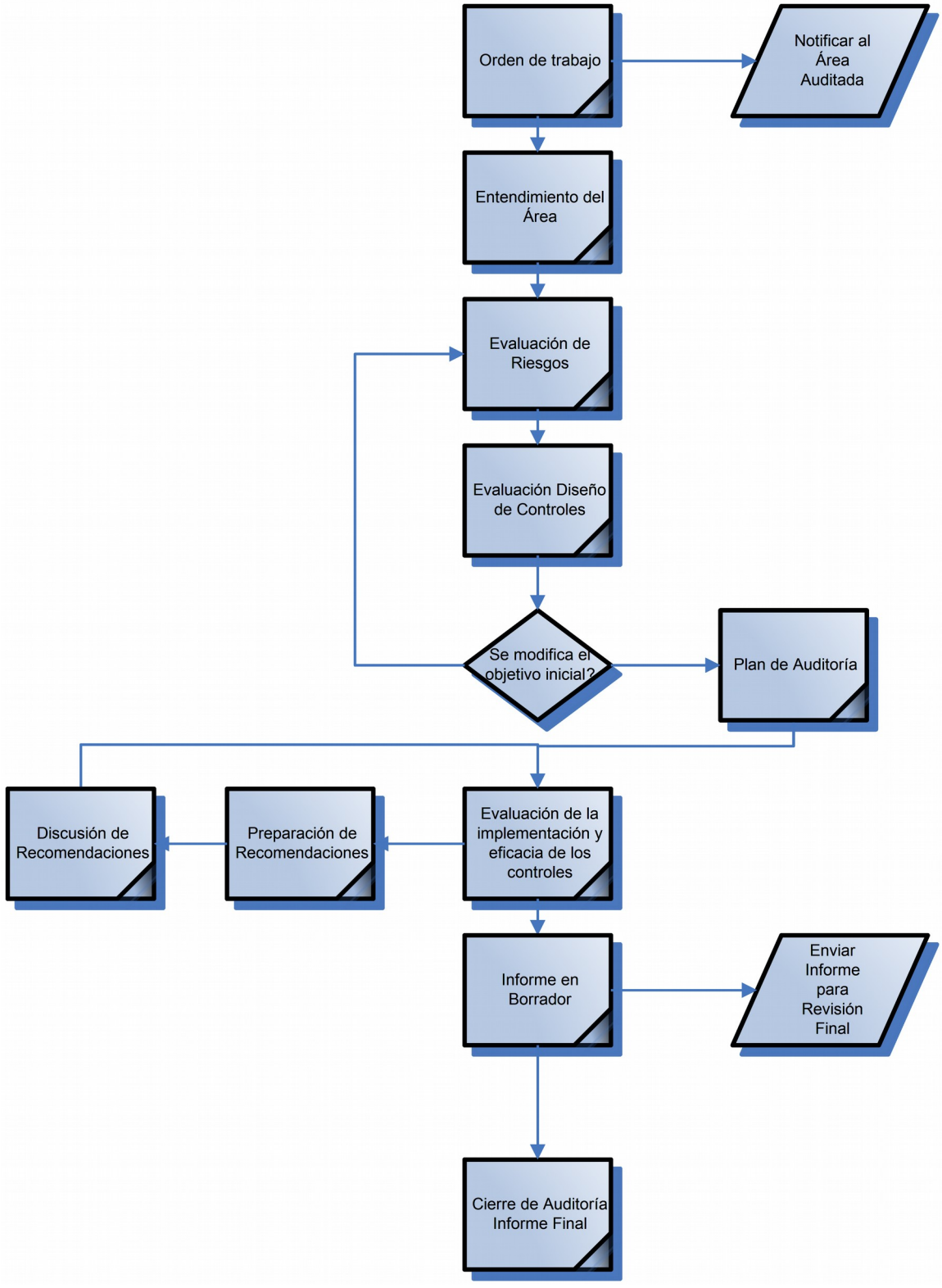

Gráfico 1: Flujo Proceso de Auditoría
Fuente: Desarrollo propio

12.2 Fases de la Metodología PEC

12.2.1 Planificación

En las últimas décadas, el rol de la auditoría interna ha venido enfocándose cada vez más en la administración de riesgos empresariales, para ello el Committee of Sponsoring Organizations of the Treadway Commision (COSO), ha generado un documento donde se describe el *Marco de Gestión de Riesgo Empresarial*. El Instituto de Auditores Internos, basado en ese documento, publicó la posición o rol del auditor interno en enfoque de Enterprise Risk Management (ERM por sus siglas en ingles) y que declaran[6]:

> *"El rol fundamental de la auditoría interna respecto al ERM es proveer aseguramiento objetivo a la junta sobre la efectividad de las actividades de ERM en una organización, para ayudar a asegurar que los riesgos claves de negocio están siendo gestionados apropiadamente y que el sistema de control interno está siendo operado efectivamente"*

[6] Instituto de Auditores Internos, *El Rol de la Auditoría Interna en la Gestión de Riesgo Empresarial*, 2004, pag 1.

Roles principales de la auditoría interna respecto al ERM	Roles legítimos de auditoría interna realizados con salvaguarda	Roles que auditoría interna no debe realizar
• Brindar aseguramiento sobre procesos de gestión de riesgo. • Brindar aseguramiento de que los riesgos son correctamente evaluados. • Evaluación de los procesos de gestión de riesgo. • Evaluación de reporte de riesgos claves. • Revisión del manejo de los riesgos claves.	• Facilitación, identificación y evaluación de riesgos. • Entrenamiento a la gerencia sobre respuesta a riesgos. • Coordinación de actividades de ERM. • Consolidación de reportes sobre riesgos. • Mantenimiento y desarrollo del marco de ERM. • Defender el establecimiento del ERM. • Desarrollo de estrategias de gestión de riesgo para aprobación de la junta.	• Establecer el apetito de riesgo. • Imponer procesos de gestión de riesgo. • Manejar el aseguramiento sobre los riesgos. • Tomar decisiones en respuesta a los riesgos. • Implementar respuestas a riesgos a favor de administración. • Responsabilidad de la gestión.

Gráfico 2: Rol de Auditoría Interna en el ERM[6]
Fuente: Instituto de Auditores Internos

Basados en este modelo, la etapa de planificación será enfocada en el conocimiento del entorno empresarial que describe los clientes que atiende, sus productos y servicios, trayectoria en el mercado, procesos de negocio y detalle de las tecnologías de información utilizadas para brindar soporte a los procesos de negocio. Con esta comprensión, el evaluador estará en posición de identificar los riesgos tecnológicos que enfrenta la organización y como éstos estarían limitándola en la consecución de los objetivos empresariales y obtención de valor por medio de la tecnología. Pero antes de seguir, es importante definir que: generar valor en una organización significa gobernar las tecnologías y alinearlas con los objetivos empresariales, obteniendo adicional a la reducción de costos, ventajas competitivas por medio de dos componentes utilidad e innovación.

Con utilidad nos referimos a los elementos que son necesarios en una organización, por ejemplo: sin electricidad, una planta de producción probablemente no operaría, de igual forma existen componentes de tecnología que hacen que las empresas simplemente funcionen. Una única inversión de tecnología, por excelente que ésta sea, no será capaz de mantener el valor indefinidamente, por lo tanto, la innovación deberá estar a tono con la industria para alcanzar o superar a los competidores. Según describe Deloitte en su artículo "Cracking the IT value code"[7], existen cuatro conductores externos y cuatro conductores internos que hacen presión sobre el modelo de gobierno de las tecnologías de información (TI) y como éstas generan valor (ver Gráfico 3). Estos conductores están acompañados de seis componentes que la organización debe alcanzar en su afán de generar valor[7]:

1. Liderazgo: ubicar la estrategia de TI junto a la estrategia del negocio, manteniendo su valor cultural, imagen corporativa y representando los intereses de la junta, inversionistas y administración.

2. Planeación: desarrollar una estrategia de TI donde se incluya la filosofía de tercerización según sea el caso, construyendo una organización corporativa de TI, generando objetivos y metas de TI corporativas que estén acordes con los objetivos del negocio u clientes de TI.

3. Recursos: identificación de recursos, determinación de presupuestos para inversiones de TI.

4. Política: crear los procedimientos fundamentales de operación de TI, estableciendo estándares, reglas, guías y definiendo la arquitectura técnica y de aplicaciones.

[7] Gentle Chris, Cracking the IT value code, Deloitte 2005.

5. Coordinación y cumplimiento: asegurando el cumplimiento de las políticas de Ti y estándares obligatorios, como regulaciones, coordinando entre actividades que demandan tecnología, suministro y administración del uso de tecnologías.

6. Seguimiento y control: benchmarking, generando sistemas de seguimiento y medición, administrando los niveles de servicio, implementando sistemas de sanción e identificando áreas de mejora.

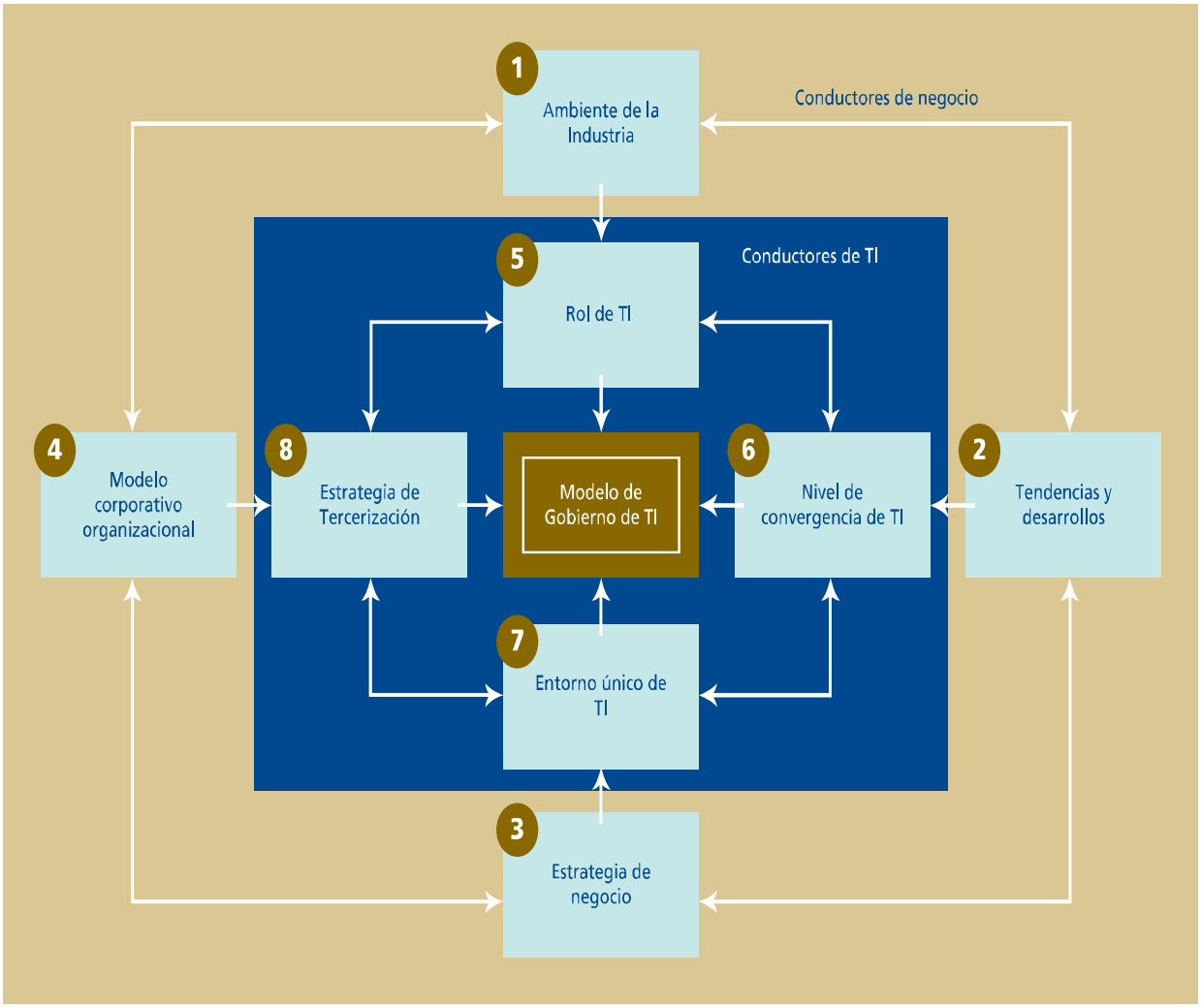

Gráfico 3: Conductores de Valor
Fuente: Deloitte

12.2.1.1 Memorando de planeación preliminar

El memorando de planeación preliminar, es el documento de partida en la labor de auditoría. Permite presentarse en la organización y anunciar e indicar a las áreas revisadas sobre el inicio de la revisión. Adicionalmente este documento define el tipo de revisión a aplicar, los objetivos y alcance formulados preliminarmente.

La idea original de la aplicación del memorando de planeación preliminar fue presentada por el profesor Rafael Palomo en el curso Enfoque de Auditoría del programa de Maestría, con el documento llamado *Orden de Trabajo Preliminar,* para la aplicación en la metodología de realización, modificaciones sobre la versión inicial con el objetivo de adaptarlo al trabajo realizado.

El memorando de planeación preliminar que se presenta en el anexo 1.1 *P-1-1 Memorando de Planeación Preliminar*, posee las siguientes secciones:

- → Encabezado del memorando: que indica la fecha y personal al que se le anuncian las pautas iniciales de la auditoría.
- → Objetivo: explica de qué se trata el memorando de planeación de auditoría.
- → Objetivo de auditoria: define el objetivo preliminar de la auditoría.
- → Alcance: marca el campo de acción donde será desarrollada la revisión. Es factible que en entornos empresariales muy amplios la revisión se limite a una ubicación física o plataforma e tecnología.
- → Contexto: brinda información o hechos relevantes que deben ser del conocimiento del personal que participa en la revisión de auditoría.
- → Tipo de auditoría:

Gobierno Corporativo	**Definición**: es una revisión de alto nivel que cubre únicamente los componentes clave de la plataforma de tecnología.

Auditoría de Sistemas	**Definición:** es una auditoria completa, donde cada aspecto del área auditada es considerado, éste incluye la revisión del diseño y operación de los controles.
Auditoría de Cumplimiento	**Definición:** es una auditoria que se encarga de validar el cumplimiento de las políticas y legislación aplicable a la Entidad.
Auditoría de Controles Clave	**Definición:** es una revisión limitada a validar el cumplimiento de los controles clave en la plataforma de Tecnología.
Revisión Analítica	**Definición:** este tipo de revisión es utilizada como complemento a una auditoría de sistemas. Da seguimiento a los controles claves identificados y los complementa con una evaluación a los datos y relación de los datos.
Auditoria de Seguimiento	**Definición:** es una corta revisión para identificar si las recomendaciones de informes anteriores han sido implementadas efectivamente.
Procedimientos Pre-acordados	**Definición:** es una revisión basada en un marco de controles pre-establecido por la entidad.

- Personal y competencias: la revisión de tecnología deberá ser realizada por personal que posee las habilidades, experiencia y competencias requeridas, para entregar un trabajo acorde a los planes de auditoría. Es importante dejar claro la cantidad de personal requerido para la revisión, así como cuales conocimientos debe tener el evaluador y comprender que éstos pueden variar dependiendo de la tecnología evaluada. A

continuación se presenta una lista[8] de competencias que podrían aplicar al ambiente evaluado y por ende al evaluador, es importante indicar que las competencias no están limitadas a la lista presentada.

Competencias del cargo	Dimensiones
1.Control de la actividad	Conoce a fondo la actividad. Controla el cumplimiento de lo establecido en el Código de Seguridad Informática Vela por el cumplimiento de todos los reclamos de clientes
2.Memoria	Retención de las informaciones esenciales Retención de detalles el mayor tiempo posible
3.Habilidades comunicativas	Tiene fluidez y facilidad en la comunicación oral Transmite en forma clara y coherente Sabe escuchar los diversos criterios Redacta de manera clara y precisa
4.Habilidad para negociar y convencer	Está al tanto de los cambios del sitio Da seguimiento y controla hasta el final los correos recibidos
5.Trabajo en equipo	Estimula el trabajo en equipo y el análisis conjunto Comparte con su grupo los problemas y dudas Busca oportunidades de trabajo conjunto que favorezcan la cohesión y espíritu de equipo
6.Saber planificarse y organizarse	Establece prioridad a sus tareas (tiene en cuenta la importancia y el tiempo para llevarla acabo) Pone fecha y orden de cumplimiento a las tareas Lleva una agenda de trabajo con todas las actividades a realizar Controla la planificación hecha
7.Creatividad	Busca alternativas a los problemas que encuentra Ante una situación nueva, formula ideas flexibles Constante iniciativa
8.Responsabilidad	Mantiene siempre seriedad y dedicación en el trabajo Vela por el cumplimiento de sus obligaciones
9.Sentido de pertenencia	Siente orgullo por su trabajo Defiende la Unidad ante todos Dedica el máximo de su tiempo y energías Alta disposición al trabajo
10.Habilidades para manejar al cliente	Tiene conocimiento de técnicas comunicativas. Se traza estrategias en el tratamiento de los clientes según su tipología.

[8] Iliana Domínguez Montes. *Elaboración del Perfil de Competencias del Especialista WEB*. http://www.gestiopolis.com/recursos5/docs/rrhh/perficompe.htm

	Se controla en situaciones críticas con el fin de ofrecer al cliente respuestas adecuadas.
11.Orientación al cliente	Conocer las informaciones generales sobre la Unidad de Negocio, estructura y funciones. Estar al tanto de cualquier modificación en los servicios que se prestan Tener una alta velocidad de respuesta. Ser éticos e informar u orientar al cliente.
12.Interés de superación	Se preocupa por recibir cursos avanzados para superarse Constantemente está retroalimentándose Accede a las vías más actualizadas de información
13.Habilidades para manejar situaciones difíciles	Tiene conocimiento de técnicas de relajación Toma medidas para disminuir la incidencia de factores estresantes Posee autocontrol en situaciones críticas de estrés con el fin de encontrar respuestas adecuadas Analiza las causas que le provocan el estrés Busca apoyo en su grupo

Tabla 1: Lista de Competencias

El auditor de Tecnología necesita poseer destrezas técnicas que le permitan comprender las vulnerabilidades en hardware, software y cómo usar herramientas de software apropiadas en la ejecución de su trabajo, posiblemente las destrezas que más va a necesitar son destrezas humanas. Después de todo, requerirá trabajar en equipo y ser capaz de interactuar con el auditado y con otros auditores, que le demandaran grandes habilidades de trabajo en equipo y relaciones interpersonales. Se dará cuenta que muchos de los pasos de la auditoría de tecnología en la evaluación de control interno no necesariamente demandan de conocimientos técnicos, por ejemplo: el entendimiento del negocio y su estructura organizacional necesitará de entrevistarse con la administración y las entrevistas son una necesidad de la auditoría.

Varios de los controles que el auditor necesitará evaluar tienen más relación con el comportamiento humano que con la tecnología, por ejemplo, varios de las vulnerabilidades de seguridad son identificadas gracias no a las auditorías en los

sistemas que están activas, si no a los procedimientos de monitoreo ejecutados por el personal de seguridad.

12.2.1.2 Fase inicial de comunicación

El memorando de planeación preliminar, nos brinda el punto de partida para nuestro trabajo de evaluación. En la fase de comunicación, anunciaremos al auditado la apertura de nuestras labores y lo introducimos en el contexto de la revisión, explicando la metodología aplicada en la revisión, los procesos de tecnología a revisar, recalcando la importancia de su participación activa durante la auditoría. En este punto es posible, si se desea, realizar un requerimiento de información inicial que permitirá avanzar en forma expedita en la fase de entendimiento del negocio. El tipo de información a solicitar dependerá del conocimiento previo que se posea de la Entidad. En caso de que ésta sea la primera vez que se realiza un trabajo de revisión, es recomendable que la información solicitada sea amplia, pues esto permitirá que la comprensión del entorno sea mejor, si es un estudio recurrente sólo debemos solicitar los cambios presentados desde la última revisión para actualizar nuestro entendimiento.
En el anexo 1.2 P-1-02 Carta Inicio Auditoría, se presenta un formato que podría ser aplicado en la auditoría.

12.2.1.3 Entendimiento del negocio y área a revisar

El procedimiento de entendimiento servirá al revisor en la familiarización con el negocio. Es importante que en este punto se identifique el tipo de organización (financiera, servicios, manufactura, medicina, seguros, construcción, etc), conocer los procesos de negocio y productos generados, identificar los funcionarios a cargo de cada proceso, establecer la distribución física de las áreas revisadas y sistemas que soportan la operación, el marco legal aplicable, estudios de auditoría anteriores relacionados con el área a revisar, entre otros.

Para la comprensión del negocio se pretende generar un formato general incluido en el anexo 1.3 P-1-03 Conocimiento del Negocio, que permita documentar el conocimiento recabado de la Entidad. Este formato cubre los siguientes puntos:

- → Historia del negocio.
- → Misión y visión.
- → Objetivos.
- → Planes futuros del negocio.
- → Procesos clave del negocio (gráfico 4).
- → Productos ofrecidos.
- → Tipo de clientes.
- → Personal y su organigrama.
- → Leyes aplicables.
- → Informes de auditorías anteriores.

Gráfico 4: Procesos de Negocio
Fuente: Desarrollo propio

Para el entendimiento del área de tecnología, se ha desarrollado un cuestionario en el anexo 1.4 P1-04 basado en las 7 áreas de potencial importancia que se presentan en el gráfico 5.

a) Administración y Planificación del Área de TI

Estructura organizacional del área, mitología de planeación a corto, mediano y largo plazo para soportar las operaciones continuas y futuras de la organización, generación de presupuestos para apoyar los planes definidos, monitoreo gerencial a las tecnologías.

b) Adquisiciones y proveedores

Procedimientos de selección y evaluación de proveedores. Administración de las relaciones con los proveedores externos en términos de niveles de servicio, continuidad de los servicios y derecho de acceso.

c) Seguridad Física, Seguridad Lógica y Acceso a los Datos

Diseño, implementación y mantenimiento de la seguridad de la información, que incluye la seguridad tanto física como lógica sobre todos las rutas de acceso a los programas y datos. Evaluación y dar prioridad a los riesgos de seguridad relevantes. Definición de los propietarios de la información, clasificando dicha información en cuanto a la seguridad necesaria, selección e implementación de herramientas y técnicas de seguridad.

d) Hardware, Redes Y Comunicaciones

Diseño, instalación y operación de hardware, redes y software de comunicación, que incluye redes de las computadoras, sistemas de voz y teléfono, transmisión de vídeo y protocolos. Esto contempla la definición de la estructura y las interrelaciones entre los componentes de la red, configurar las ubicaciones físicas de los archivos y el equipo, y planear la capacidad operativa y las habilidades para cumplir las necesidades actuales de la red mientras se mantiene la flexibilidad de modificar el sistema para responder a las necesidades futuras.

e) Continuidad de las Operaciones

Desarrollo de un plan que abarque toda la entidad para mantener y/o restaurar las operaciones de negocios, en el caso de un desastre, dentro de un esquema de tiempo que sea aceptable para la organización.

f) Mantenimiento e implementación de Sistemas de Información

Procedimientos de selección o desarrollo, implementación y mantenimiento de los sistemas de aplicación utilizados para soportar las operaciones del negocio. E identificación del alineamiento de estos desarrollos con los planes estratégicos de la organización.

g) Software y Bases de Datos

Administración de la arquitectura y mantenimiento de la información en términos de definir y conservar la estructura de los datos de los archivos maestros, datos de las transacciones y datos de la organización. Sostenimiento del sistema de administración de la base de datos (o su equivalente). Selección, implementación y mantenimiento del software necesario de los sistemas (sistemas operativos), que incluye los parámetros que configuran y que controlan dicho software. Desarrollar y monitorear los cambios en el software del sistema, que incluye las actualizaciones de proveedores.

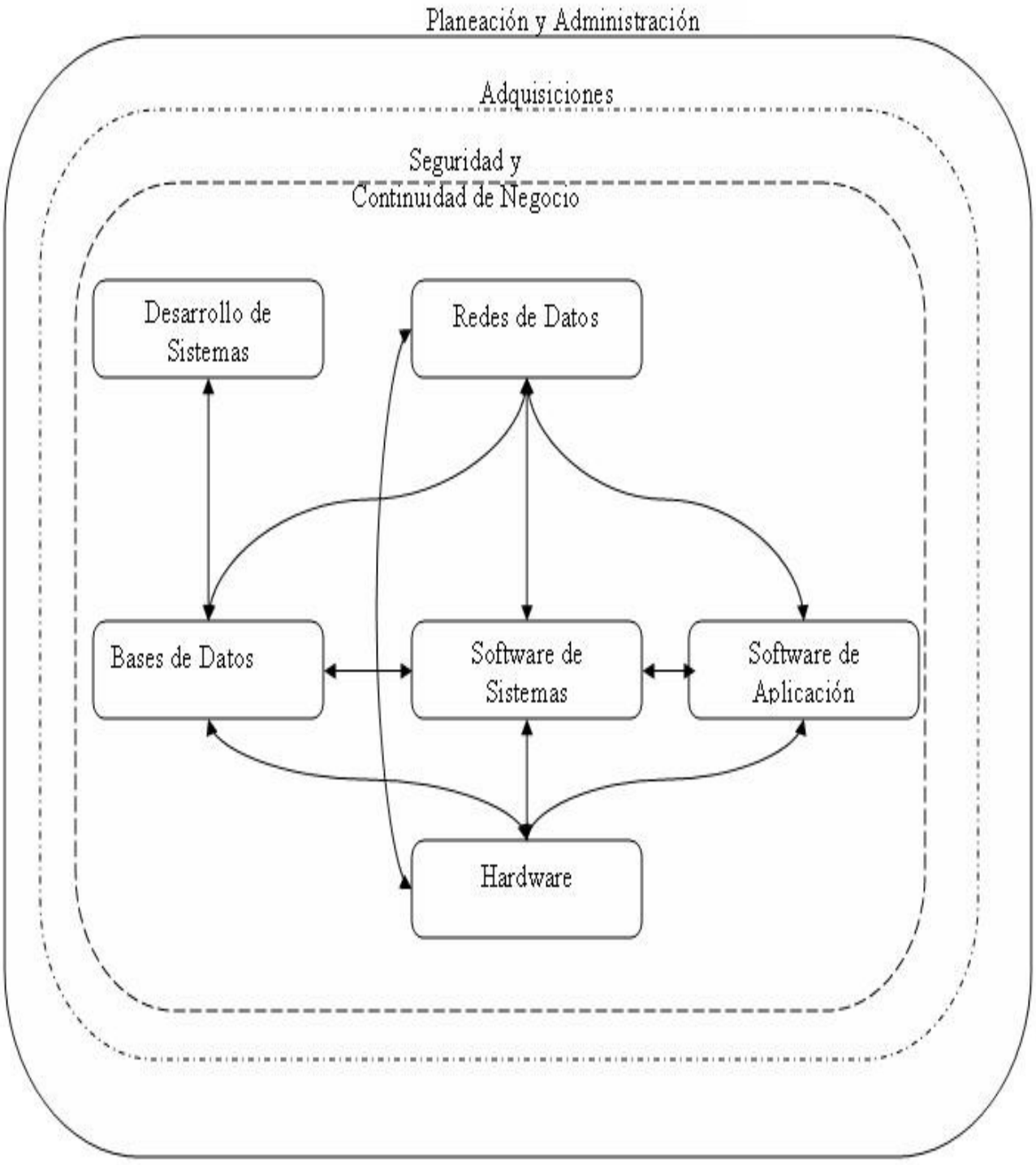

Gráfico 5: Áreas de Potencial Importancia
Fuente: Desarrollo propio

12.2.1.4 Evaluación de riesgos[9]

Una evaluación de riesgos le permitirá a la organización identificar los posibles daños que podrá sufrir como resultado de la materialización de los peligros que afronta.

Algunas organizaciones poseen dentro de su estructura organizacional, la función de administración de riesgos. El rol del departamento de administración de riesgos es usualmente trabajar en la identificación, evaluación y control de las perdidas potenciales que la organización podría tener como resultado de eventos que aún no se han presentado. Los beneficios de la evaluación de riesgos no son sólo de tipo costo-beneficio, de hecho, el departamento de administración de riesgo puede tener una comprensión del giro del negocio, sus objetivos, el ambiente en que se desarrolla y una apreciación de los eventos contingentes que podría afronta la empresa en la consecución de sus objetivos y estará en la capacidad de avaluar dichos riesgos y proponer planes de mitigación que coordinará y ejecutará.

Sin embargo, existen organizaciones que aun no poseen un departamento de administración de riesgos. Estas organizaciones tienen dos caminos para atacar el asunto de la evaluación de riesgos, el primero es la contratación de un consultor externo para realizar esta tarea. La segunda es elegir a un funcionario de la organización y enseñarle como ejecutar un proceso de evaluación de riesgos. No es factible definir cúal de las dos opciones es la mejor, para ello es importante realizar una evaluación de la organización y su entorno para determinar qué es lo más beneficioso. Sin importar cual de los dos caminos tome la organización, es importante definir que existen diferentes metodologías para la evaluación de riesgos, sin embargo, éstas se dividen básicamente en cuantitativas y cualitativas.

[9] Para la definición del proceso de evaluación de riegos se ha utilizado como fuente el documento NIST Special Publication 800-30 referente a la evaluación de riesgos de seguridad. Se aplicaron modificaciones a dicha metodología para adaptarla a un proceso de evaluación de riesgos que aplique a toda la plataforma de tecnología de la Entidad y no sólo a seguridad.

A continuación se presenta una tabla[10] resumen de las ventajas e inconvenientes de cada modelo y seguidamente una descripción de cada modelo.

	Cuantitativo	Cualitativo
Ventajas	– Se asignan prioridades a los riesgos según las repercusiones financieras; se asignan prioridades de los activos según los valores financieros. – Los resultados facilitan la administración del riesgo por el rendimiento de la inversión en seguridad. – Los resultados se pueden expresar en terminología específica de administración (por ejemplo, los valores monetarios y la probabilidad expresados como un porcentaje específico). – La precisión tiende a ser mayor con el tiempo a medida que la organización crea un registro de historial de los datos mientras gana experiencia.	– Permite la visibilidad y la comprensión de la clasificación de riesgos. – Resulta más fácil lograr el consenso. – No es necesario cuantificar la frecuencia de las amenazas. – No es necesario determinar los valores financieros de los activos. – Resulta más fácil involucrar a personas que no sean expertas en seguridad o en informática.
Inconvenientes	– Los valores de repercusión asignados a los riesgos se basan en las opiniones subjetivas de los participantes. – El proceso para lograr resultados creíbles y el consenso es muy lento. – Los cálculos pueden ser complejos y lentos. – Los resultados sólo se presentan en términos monetarios y pueden ser difíciles de interpretar por parte de personas sin conocimientos técnicos. – El proceso requiere experiencia, por lo que los participantes no pueden recibir cursos fácilmente durante el mismo.	– No hay una distinción suficiente entre los riesgos importantes. – Resulta difícil invertir en la implementación de controles porque no existe una base para un análisis de costo-beneficio. – Los resultados dependen de la calidad del equipo de administración de riesgos que los hayan creado.

[10] Microsoft Corporation, *Guía de administración de riesgos de seguridad,* http://www.microsoft.com/latam/technet/articulos/adminriesgos/srsgch02.mspx.

12.2.1.4.1 Análisis cuantitativo de riesgos

Este enfoque se concentra en dos asuntos: la probabilidad de que un evento ocurra y las pérdidas que se podrían generar si el evento se presenta. A partir de estos dos elementos se produce una figura multiplicando las pérdidas potenciales (medidas en términos monetarios) por su probabilidad (medida en porcentaje). Claramente el número más alto que un riesgo posea, más serio será para la organización. Es posible clasificar los eventos contingentes y tomar acciones sobre los riesgos más importantes.

El problema con este tipo de análisis de riesgos está usualmente asociado con la subjetividad de la evaluación y lo poco precisa que ésta es en ocasiones. Adicionalmente, los controles tienen que afrontar un número de eventos potenciales y estos por sí solos están relacionados con otros eventos. Una clasificación detallada podría hacer difícil de identificar las relaciones y guiar hacia una pobre decisión sobre el control, por ello esta metodología no es recomendada. A pesar de esto es importante indicar que existen organizaciones que han adoptado este método exitosamente.

12.2.1.4.2 Análisis de Riesgo cualitativo

Es un enfoque muy utilizado debido a que la probabilidad numérica no es requerida y sólo la estimación de pérdidas potenciales es utilizada. Los análisis cualitativos utilizan un número de eventos interrelacionados, en el cual para cada objetivo de negocio se presentan sus amenazas, vulnerabilidades e impactos.

Objetivos incluidos en el alcance:

El primer paso es identificar los objetivos de la organización. Según se desee será una buena práctica identificar los activos tecnológicos que apoyan la consecución de cada objetivo y con esto se estará definiendo el marco de acción. Los activos se definen como cualquier elemento que represente valor para la organización que incluye activos intangibles como la reputación de la

empresa e información digital y activos tangibles como la infraestructura física de servidores y comunicaciones.

Amenazas:

NIST[11] define una amenaza como un suceso con posibilidad de dañar el sistema. Las repercusiones derivadas de una amenaza normalmente se definen con conceptos como confidencialidad, integridad y disponibilidad. Las amenazas son accionadas por un intento apuntado en la explotación intencional de una vulnerabilidad o una situación que pueden accionar accidentalmente una debilidad. Una amenaza por sí sola no es un riesgo si no existen flaquezas ante dicha amenaza que puedan provocar un daño.

Existen tres fuentes de amenazas[11]:

1. Amenazas naturales: inundaciones, terremotos, tornados, deslizamientos, avalanchas, tormentas eléctricas y otros eventos parecidos.
2. Amenazas humanas: eventos que son activados o causados por humanos, como se muestran en la tabla 2.
3. Amenazas del ambiente: fallas de corriente por períodos prolongados, polución, químicos, goteras de líquidos, entre otros.

Amenaza	Motivador	Acciones
Hacker, cracker	– Desafío. – Ego. – Rebelión.	– Hacking. – Ingeniería Social. – Intrusión en los sistemas. – Accesos no autorizados.
Crimen computacional	– Destrucción de información. – Divulgación ilegal de Información. – Ganancias económicas. – Alteración de datos no autorizada.	– Crimen computacional como acecho cibernético. – Actos fraudulentos como personificación o intercepción. – Soborno por información. – Spoofing. – Intrusión en los sistemas.
Terrorismo	– Chantaje. – Destrucción.	– Terrorismo/bombas. – Guerra por información.

[11] Gary Stoneburner. *Risk Management Guide for Information Technology Systems*, NIST Special Publication 800-30.

	– Explotación. – Venganza.	– Ataque de sistemas como denegación de servicio. – Penetración de sistemas.
Espionaje industrial	– Ventaja competitiva. – Espionaje económico.	– Explotación económica. – Robo de información. – Intrusión en la privacidad personal. – Ingeniería Social. – Penetración de sistemas. – Accesos no autorizados.
Internos (empleados mal entrenados, contrariedades, malévolos, negligentes, deshonestos, o despedidos)	– Curiosidad. – Ego. – Inteligencia. – Ganancias económicas. – Ego. – Ego. – Venganza. – Errores sin intención u omisiones.	– Asalto de un empleado. – Chantaje. – Inspeccionar información confidencial. – Abuso de las tecnologías. – Fraude y Robo. – Soborno por información. – Falsificación de datos. – Código malicioso. – Venta de información personal. – Pulgas de los sistemas. – Intrusión en los sistemas. – Sabotaje. – Accesos no autorizados.

Tabla 2: Amenazas Humanas

Vulnerabilidades[11]*:*

Un defecto o una debilidad en procedimientos, diseño o implementación de los controles internos que podrían ocasionar que el activo o los objetivos sean afectados por un fenómeno perturbador accionado en forma accidental o intencional.

Las vulnerabilidades técnicas y no técnicas asociadas a la plataforma de tecnología y su ambiente pueden ser identificadas por medio de los siguientes métodos:

→ Cuestionarios: para obtener información en el proceso de evaluación de riesgos, es posible desarrollar un cuestionario de control interno para identificar los controles y su administración. Este cuestionario deberá ser aplicado al nivel gerencial y al nivel operativo que brinda servicios a la plataforma de tecnología pues de esta forma se obtendrá una mejor

comprensión. En este proceso puede aplicar el cuestionario incluido en el anexo 1.4 P-1-04 Conocimiento del área de TI.

→ Entrevistas: entrevistas con el personal de tecnología y la administración le permitirán obtener información útil para la evaluación de riesgos. En el proceso de entrevista podrá aplicar los cuestionarios de control interno. Otra ventaja de las entrevistas es que le permitirán hacer observaciones sobre los procedimientos de seguridad física, ambiental y de operación.

→ Revisión de documentos: documentos de políticas, procedimientos, leyes, reglamentos, manuales, entre otros, le dará un buen panorama sobre los controles de TI diseñados y aplicados por la Entidad.

→ Uso de herramientas de escaneo: proveen información técnica sobre la seguridad de la plataforma tecnológica, los componentes de sistema operativo y base de datos utilizados y sus configuraciones.

Impacto:

Un impacto es la materialización de una vulnerabilidad por una amenaza que tendrá una repercusión en el activo o en los objetivos de la organización. Estos impactos se identifican y en cuanto sea posible se les asigna un valor monetario.

Evaluación de Riesgo:

El riesgo deberá ser evaluado para identificar los daños potenciales que éste pueda causar a la organización. El riesgo debe ser calificado según su impacto y qué tan vulnerable es la organización frente a este riesgo, de esta forma será posible clasificarlos numéricamente y concluir para cada riesgo si es aceptable o si requiere de implementación de controles.

Controles:

Los controles son las medidas para reducir el potencial de pérdida o minimizar los riesgos. Los controles se clasifican en tres grupos[12]:

[12] Definiciones tomadas de la presentación *Tipos de controles en los sistemas,* recibida en el curso PF-2563 Auditoría de Sistemas en Operación.

Preventivos: minimizan o reducen que un evento o actividad no deseada ocurra en la preparación, entrada y proceso de los datos que van a ser ingresados al computador

Detectivos: revelan que alguna actividad está fuera de parámetros en el momento de un proceso determinado.

Correctivos: proveen procedimientos e instrucciones apropiadas para corregir los errores u otros eventos que han sido detectados o se han producido.

Es importante que cada control implementado sea costo-beneficio para la organización. El principio se basa en que el costo del control no debe ser más alto que el costo del impacto.

12.2.1.4.3 Descripción de la herramienta

Es importante que antes de iniciar el análisis de riesgos se defina claramente el alcance de éste y a su vez que el alcance definido esté alineado con el objetivo de auditoría preliminar del papel P-1-01 Memorando de Planificación Preliminar.

La herramienta propuesta en el Anexo 1.5 para el proceso de análisis de riesgos se compone de 5 pasos:

1. *Objetivos y activos:*

   Durante las entrevistas con la administración y aplicación de los cuestionarios P-1-03 Conocimiento del Negocio y P-1-04 Conocimiento del área de TI, se formará un panorama general sobre la organización y su ambiente. De este proceso es importante que se identifiquen los objetivos del negocio, pues ellos serán la base para el proceso de evaluación de riesgos, en caso de que la organización no haya definido los objetivos del negocio, éste es un buen momento para que la administración defina dichos objetivos y las tareas que realizarán para llevarlos a cabo. Por lo general, los objetivos se expresan como un incremento en las ganancias, sin embargo, esos son el

resultado de incrementar las ventas de un producto “x” en un segmento de mercado “y”.

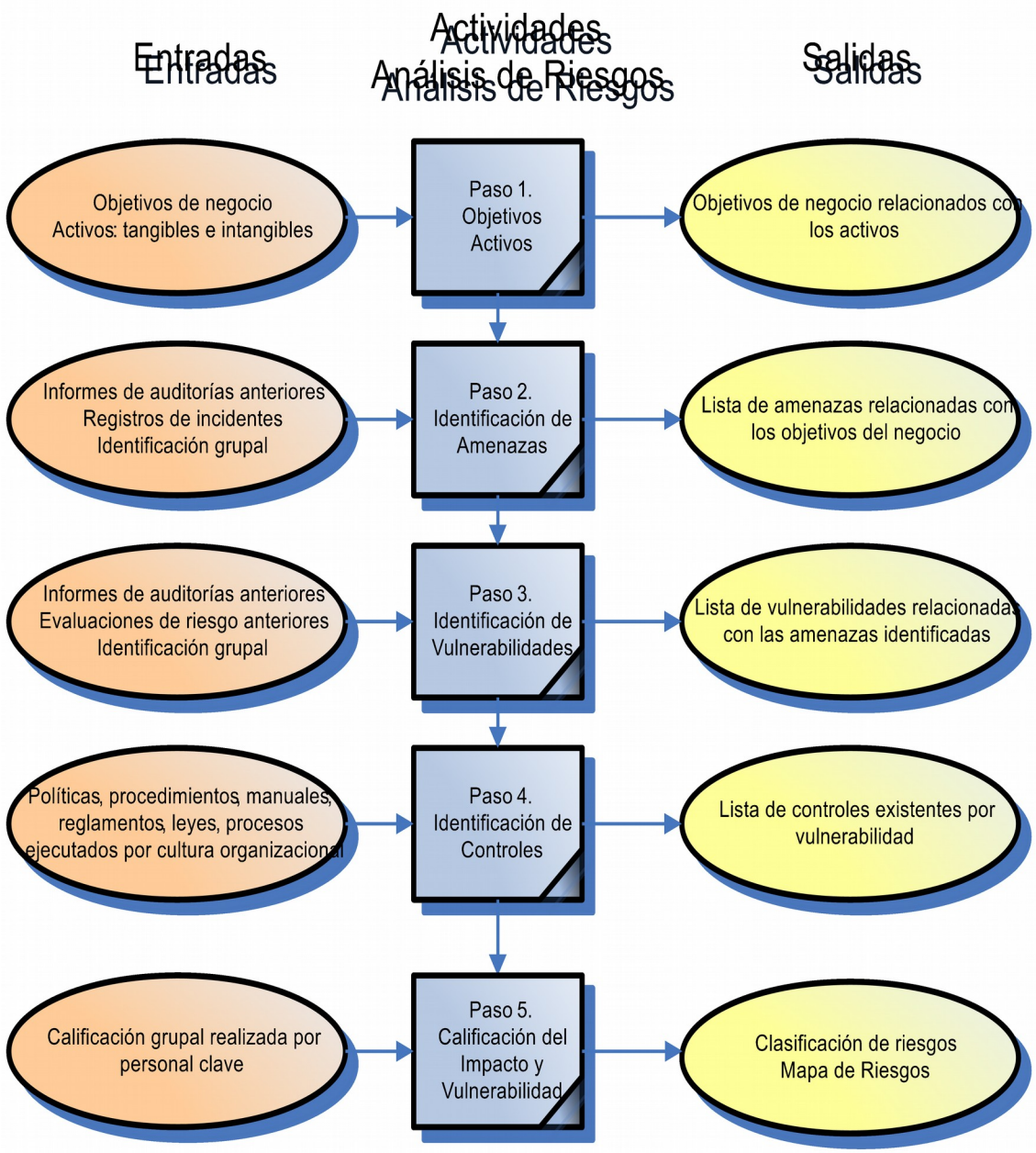

Gráfico 6: Metodología Análisis de Riesgos
Fuente: Desarrollo propio

Los objetivos definidos deben ser específicos, medibles, reales y definidos en el tiempo. Los objetivos identificados se deben listar en la columna “Objetivo de Negocio” de la herramienta de análisis de riesgos.

Una vez identificados los objetivos, relacione los activos de tecnología que soportan dichos procesos en la columna “Activos TI”. Es recomendable que esta relación de activos y objetivos la realice en conjunto con el nivel gerencial de área de tecnología.

2. *Identificación de amenazas y vulnerabilidades:*

La identificación de amenazas y vulnerabilidades es factible realizarla en un solo paso, sin embargo, para efectos ilustrativos en el gráfico 6 donde se observa el flujo de la metodología, se incluyen por separado.

Para hacer este proceso de identificación, es importante que se conforme un equipo multidisciplinario que se encargue de analizar cuáles amenazas enfrenta la organización y cuáles vulnerabilidades existen ante dichas amenazas. Para cada amenaza es necesario crear una fila y relacionar el objetivo y sus vulnerabilidades. Esta información se ingresa en las columnas llamadas “Amenaza” y “Vulnerabilidad”.

La calidad de los controles que implemente la organización será el reflejo de la calidad del ejercicio de identificación de amenazas y vulnerabilidades.

3. *Identificación de controles:*

El objetivo de este paso es identificar los controles implementados por la organización para hacer frente a las vulnerabilidades identificadas. Es importante incluir los controles que la organización está por implementar o ya tiene identificados, para que la lista de controles sea lo más completa posible.

Como fuente de controles es recomendable hacer una revisión documental de leyes aplicables a la organización, políticas, procedimientos, normas, manuales de operación o de usuario, entre otros y realizar entrevistas con los dueños de proceso evaluado, para validar los controles incluidos en la lista verificar si existen controles que no hemos incluido. Es importante tomar en cuenta que algunas organizaciones pueden no tener documentación y eso no significa que no posean controles implementados, para estos casos es mejor hacer una entrevista con el dueño de proceso e identificar los procedimientos de configuración, administración y operación utilizados.

4. Calificación del impacto y la vulnerabilidad:

Al igual que el proceso de determinación de amenazas y vulnerabilidades, la calificación deberá ser realizada por un equipo de personas donde cada integrante votará individualmente y al final se obtendrá un promedio de las calificaciones individuales.

Para la calificación numérica hay que tener en cuenta la relación existente entre el impacto de la vulnerabilidad y los controles existentes, entre más alto sea el valor asignado al rubro de vulnerabilidad significa que menos controles existen para compensar la amenaza, por otra parte entre más elevado sea el número del impacto significa que la organización podría estar comprometiendo su continuidad de operación y presentar pérdidas económicas significativas.

Para realizar la calificación numérica se definieron 5 categorías:

Impacto	Valor	Vulnerabilidad	Valor
Muy Alta	1	Muy Alta	100
Alta	0.8	Alta	80
Media	0.6	Media	60
Baja	0.4	Baja	40
Muy Baja	0.2	Muy Baja	20

Tabla 3: Calificación Numérica Impacto Vulnerabilidad

La calificación del riesgo total, se obtiene multiplicando el valor asignado al impacto por el valor asignado a la vulnerabilidad y se grafica en un mapa de riesgo:

Nivel de riesgo	Límite inferior	Límite superior
Muy Alta	80	100
Alta	60	79
Media	40	59
Baja	20	39
Muy Baja	1	19

Gráfico 7: Rangos por Nivel de Riesgo
Fuente: Desarrollo propio

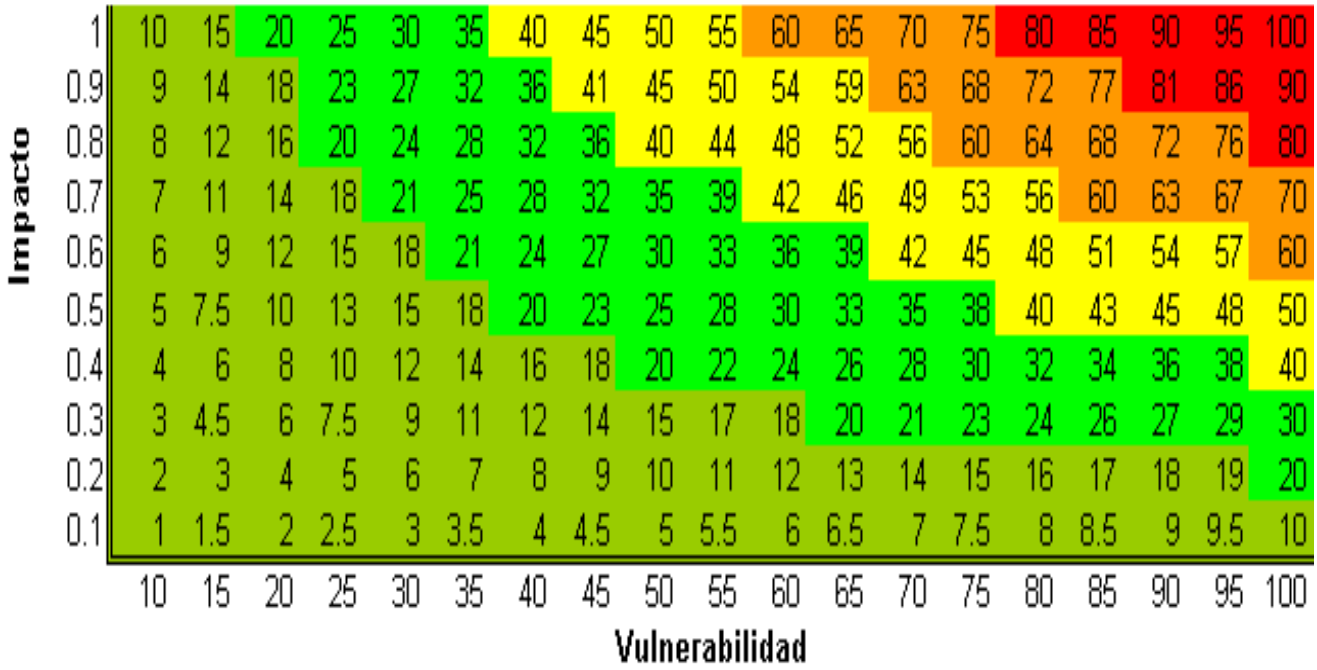

Gráfico 8: Mapa de Riesgos
Fuente: Desarrollo propio

12.2.1.5 Programa de auditoría

El programa de auditoría es necesario para realizar una auditoría efectiva y eficiente. El programa es una guía de varias pruebas que el auditor deberá ejecutar dentro del alcance de la auditoría para determinar si los controles diseñados para mitigar riesgos están funcionando según lo planeado. Basado en los resultados de las pruebas, estará en capacidad de opinar sobre la suficiencia y validez de los controles sobre el proceso evaluado.

El programa de auditoría también puede complementar la administración de la auditoría y asignación de recursos. El administrador de la auditoría puede por ejemplo, estimar el total de horas requeridas para ejecutar la auditoría basado en el tiempo estimado de cada paso ejecutado o control evaluado. Otro beneficio del uso de programa de auditoría es que proveen consistencia en las pruebas ejecutadas en auditorías semejantes, de un ciclo hacia el siguiente.

Durante la fase de planeación de la auditoría, los programas de auditoría utilizados en auditoría anteriores pueden ser utilizados como pasos base a ejecutar durante la auditoría actual. Esto no aplica en los casos donde el proceso no ha sido revisado anteriormente o posee cambios significativos; en esos casos el programa de auditoría deberá ser creado.

Es recomendable que se utilice un marco de control para la definición de los objetivos y criterios de auditoría, pues este será su apoyo en el planteamiento de recomendaciones y le permitirá evaluar el proceso actual contra el nivel que debería tener la organización. Existen diferentes tipos de marcos de control por ejemplo, regulaciones legales a las que la organización está sujeta, estándares internacionales, mejores prácticas o sus propias prácticas de control interno. Es importante que seleccione el marco de control apropiado para el proceso evaluado, pues este marco de control, como su nombre lo indica, le definirá el “set” de controles que la organización debería tener implementados y en caso de que alguno de los controles no esté presente, esto le generará una recomendación a la administración.

Para la realización del programa de auditoría, se incluye en el anexo 1.6 *E-1-1 Programa de Auditoría*, un formato que le permitirá documentar los objetivos de control y sus criterios en la hoja llamada "Objetivos y Criterios" y posteriormente formular los procedimientos de auditoría para cada criterio seleccionado. Es importante indicar que la cantidad de objetivos y criterios a incluir dependerá del proceso evaluado y de la experiencia del auditor.

En el diseño de las pruebas es factible que se desee realizar muestras para probar los controles, por ejemplo, para la validación de procedimientos de creación de usuarios deseará seleccionar una muestra de los accesos otorgados durante el período evaluado y no la totalidad de los accesos otorgados. En la selección del tamaño de la muestra existen factores a contemplar como es el porcentaje de error esperado, sin embargo, en la tabla 4 se presenta un tamaño de muestra[13] comúnmente usado por compañías y auditores en la prueba de controles basado en la frecuencia de ejecución del control.

Naturaleza del Control	Frecuencia de Ejecución	Tamaño Mínimo de Muestra*
Manual	Varias veces al día	25
Manual	Diario	25
Manual	Semanal	5
Manual	Mensual	2
Manual	Trimestral	2
Manual	Anual	1
Automático	Pruebe una aplicación de la actividad de control.	
* Asumiendo que los controles son efectivos		

Tabla 4: Tamaño de Muestra

12.2.2 Evaluación del control

[13] IT Governance Institute, *IT Control Objectives for Sarbanes-Oxley*, Segunda Edición Setiembre 2006.

La evaluación del control es el proceso de ejecución de guías de auditoría y coordinación del trabajo de campo con el personal auditado. Durante este proceso el revisor aplicará las pruebas para determinar si el control está funcionando de acuerdo al diseño realizado o si por el contrario existen áreas donde se deben aplicar nuevos controles o modificar los existentes. Es de esperar que la organización haya diseñado controles que nunca llegaron a ser implementados y por presión de revisiones, su implementación será realizada. El auditor debe obtener evidencia suficiente, relevante y competente para soportar sus conclusiones sobre el control evaluado. Esta evidencia debe ser documentada en los papeles de trabajo. No se incluye como objetivo de este proyecto la definición de cómo documentar los papeles de trabajo u estándares para la documentación, se presentan formatos que podrán ser aplicados y modificados a las necesidades de cada proceso.

12.2.3 Comunicación de resultados

Las deficiencias identificadas durante la evaluación del control, pueden ser documentadas en el formato C-1-01 Formato Recomendaciones y revisadas con el auditado, para obtener su opinión al respecto. Este formato incluye como principales campos los siguientes:

- → Condición: es la descripción en detalle de la situación observada, que le explica al lector claramente cuál es la deficiencia. Las recomendaciones deben ser redactadas en un lenguaje comprendido por cualquier lector, evite utilizar términos muy técnicos que confundan o no introduzcan al espectador en la deficiencia.

- → Criterio: es una referencia al punto del marco de control utilizado, en donde la entidad no ha cumplido con el objetivo de control. Esta referencia le da peso a su observación, si el marco de control utilizado es un estándar ISO o una ley, es probable que la administración le resulte

más interesante su observación y por ende la implementación que si el criterio aplicado fuese únicamente su juicio y experiencia profesional.

→ Causa: durante la ejecución del trabajo de campo y las pruebas de auditoría, es relevante que una vez identificada la deficiencia, busque su origen, pues la recomendación debería estar enfocada en eliminar de raíz la deficiencia.

→ Efecto: aquí se describe el riesgo que enfrenta la organización por no tener el control implementado o funcionando correctamente. Es factible que se apoye en el análisis y riesgo inicial para la definición de éste.

→ Recomendación: para la recomendación es importante que analice la causa de la deficiencia y enfoque las acciones de solución para eliminar esta causa. Adicionalmente las recomendaciones deben ser realistas y costo-efectivas para la organización. No tendría razón que se recomiende un control cuyo costo de implementación sea más elevado que el impacto del mismo.

Finalizadas todas las recomendaciones puede compilarlas y realizar un resumen de los resultados que debe ser presentado en una reunión final de auditoría, a la función administrativa del área auditada previamente de presentar el informe a la junta directa u organismo de mayor rango en la organización. Antes de discutir las observaciones, el revisor deberá asegurarse de los siguientes puntos:

→ La información de las recomendaciones es correcta y posee evidencia de soporte.

→ Revisar que las recomendaciones planteadas son costo-efectivas para la organización, en caso de no serlo, debe buscar otro tipo de recomendación negociada con el área auditada.

→ Sugerir fechas de implementación para las recomendaciones dadas.

Durante la discusión del informe debe obtener los comentarios de la administración indicando cuál sería su plan de acción para solucionar la deficiencia y la fecha de implementación. Es importante indicar que algunas organizaciones prefieren obtener una copia de las recomendaciones para realizar un plan de acción e incorporarlo en el plan de trabajo anual, por lo tanto, en estos casos no obtendrá los comentarios en forma inmediata y deberá incluir una nota en las observaciones que indique el estado de las observaciones (en borrador y sin comentarios) para evitar que el área auditada o la organización, tomen dicho documento como la versión final del informe de auditoría.

Obtenidos los comentarios deberá preparar el informe final de auditoría. A continuación se presenta una sugerencia de qué debería incluir este informe. No se adjunta un formato de ejemplo porque este proceso varía sustancialmente de organización en organización.

Estructura del informe:

→ Introducción.
→ Declaración de los objetivos y alcance de la auditoría.
→ Período cubierto por la auditoría.
→ Descripción sobre los tipos de procedimientos de auditoría aplicados.
→ Conclusión y opinión del revisor sobre si los controles evaluados son adecuados acorde a los objetivos fijados y las necesidades de la entidad.
→ Reservas, limitaciones o calificaciones del revisor referente a la auditoría.
→ Detalle de las observaciones y recomendaciones.

13 Capítulo 2: Aplicación de la Metodología PEC

Es importante indicar que los papeles de trabajo desarrollados durante el proceso de auditoría, no serán adjuntados como anexos por lo sensitiva que es la información allí capturada.

13.1 Planificación

13.1.1 Memorando de planeación preliminar

La auditoría informática de seguridad es la revisión y la evaluación de los controles y procedimientos de la organización tendientes a brindar integridad, confidencialidad y disponibilidad al procesamiento de la información, a fin de que por medio del señalamiento de cursos alternativos se logre una utilización más eficiente y segura de esta, que servirá para una adecuada toma de decisiones.

La información y los procesos, sistemas y redes que le brindan apoyo, constituyen importantes recursos de la empresa. La confidencialidad, integridad y disponibilidad de la información pueden ser esenciales para mantener la ventaja competitiva, el flujo de fondos, la rentabilidad, el cumplimiento de las leyes y la imagen comercial.

Las organizaciones y sus redes y sistemas de información, se enfrentan en forma creciente con amenazas relativas a la seguridad, de diversos orígenes, que incluye el fraude asistido por computadora, espionaje, sabotaje, vandalismo, incendio o inundación. Daños tales como los ataques mediante virus informáticos, "hacking" y denegación de servicio se han vuelto más comunes, ambiciosos y crecientemente sofisticados.

La dependencia de las organizaciones con respecto de los sistemas y servicios de información denota que ellas son más vulnerables a las amenazas concernientes a seguridad. La interconexión de las redes públicas y privadas y el uso compartido de los recursos de información incrementa la dificultad de lograr

el control de los accesos. La tendencia hacia el procesamiento distribuido ha debilitado la eficacia del control técnico centralizado.

Muchos sistemas de información no han sido diseñados para ser seguros. La seguridad que puede lograrse por medios técnicos es limitada y debe ser respaldada por una gestión y procedimientos adecuados. La identificación de los controles que deben implementarse requiere una cuidadosa planificación y atención a todos los detalles. La administración de la seguridad de la información, exige, como mínimo, la participación de todos los empleados de la organización. También puede requerir la participación de proveedores, clientes y accionistas. Asimismo, puede requerirse el asesoramiento experto de organizaciones externas. Los controles de seguridad de la información resultan considerablemente más económicos y eficaces si se incorporan en la etapa de especificación de requerimientos y diseño.

Por todo lo anterior, para el proceso de auditoría en cuestión, se ha definido como objetivo de auditoría:

> *"Determinar la suficiencia y validez de controles de seguridad en el entorno de tecnología de información".*

Aunque no se menciona en la metodología, se han determinado los siguientes factores críticos de éxito para lograr una ejecución satisfactoria de este proceso de auditoría:

- → Política de seguridad, objetivos y actividades de tecnología que reflejen los objetivos de la empresa.

- → Una estrategia de implementación de seguridad que sea consecuente con la cultura organizacional.

→ Apoyo y compromiso manifiestos por parte de la gerencia.

→ Claro entendimiento por parte de la administración de los requerimientos de seguridad, la evaluación de riesgos y la administración de los mismos.

→ Comunicación eficaz de los temas de seguridad a todos los gerentes y empleados.

→ Distribución de guías sobre políticas y estándares de seguridad de la información a todos los empleados y contratistas.

→ Instrucción y entrenamiento adecuados.

→ Un sistema integral y equilibrado de medición que se utilice para evaluar el desempeño de la gestión de la seguridad de la información y para brindar sugerencias tendientes a mejorarlo.

13.1.2 Fase inicial de comunicación

Para el inicio de la revisión se le comunicó al Jefe del Área de Tecnología el inicio de nuestra labor de revisión el día 15 de febrero del 2007 para finalizar el 27 de abril del 2007. Este inicio fue documentado utilizando el formato P-1-02 Carta Inicio Auditoría.

13.1.3 Entendimiento del negocio y área a revisar

Ejecutado el cuestionario de entendimiento del negocio se definió el siguiente perfil de organización:

13.1.3.1 Reseña

La Entidad se constituyó en la compañía que jurídicamente es hoy, en el año 1979. Sin embargo, su verdadero origen como entidad prestadora de servicios de avalúo y asesoría de construcción se remonta al año 1968, donde sus accionistas se asociaron bajo el nombre de Consultores Asociados S.A., para ofrecer a la industria en general la experiencia que a través de once años de trabajo en procesos de avalúo y estratégicos de construcción que habían acumulado en prestigiosas empresas nacionales.

Desde el día de su fundación hubo el acuerdo expreso y muchas veces comentado entre los socios fundadores, que los más altos principios éticos regirían todos los actos de la nueva compañía.

No fue una decisión fácil de implementar a lo largo de la vida. La gran contratante de consultorías en ese momento era el Estado y los principios éticos de la naciente empresa chocaban fácilmente con las costumbres de contratación de los representantes del Estado.

Prevalecieron los principios éticos y se resolvió vivir del incipiente y pequeño sector privado donde dichos principios fueron apreciados y justamente remunerados.

Otro principio que moldeó el desarrollo de la compañía fue el de “no endeudamiento”. Los mercados para consultoría de construcción parecen demasiado inestables e in-pronosticables para adquirir deudas a pagar con inciertos ingresos de expectativas futuras.

Ya por los años 1976 los socios y muy principales gestores de la actividad de la compañía se habían especializado en campos un poco diferentes. Fue por esto que se juzgó prudente hacer una separación de actividades y así surgió Consultores Asociados S. en C la cual se transformo en la firma Consultores y Asociados S.A.

El contar durante más de 20 años con sólo el sector privado como cliente y la filosofía de “el no endeudamiento” limitó el ritmo de crecimiento de la compañía.

Hoy sin embargo, ambos principios, el de la más estricta ética y el de no endeudamiento, han dado frutos que ni sospecharon sus fundadores y que

proyectan la compañía en el siglo 21 no como la más grande en el sector, pero sí como la más sólida y reputada.

Cada una de las divisiones de Consultores Asociados S.A., tiene productos claramente identificados, y cuenta con el capital humano y materiales en cada uno de esos campos de especialización.
Los clientes tienen acceso inmediato a la variada experiencia acumulada por los profesionales para la solución de sus preocupaciones en cada una de las áreas de servicios.

13.1.3.2 Organigrama

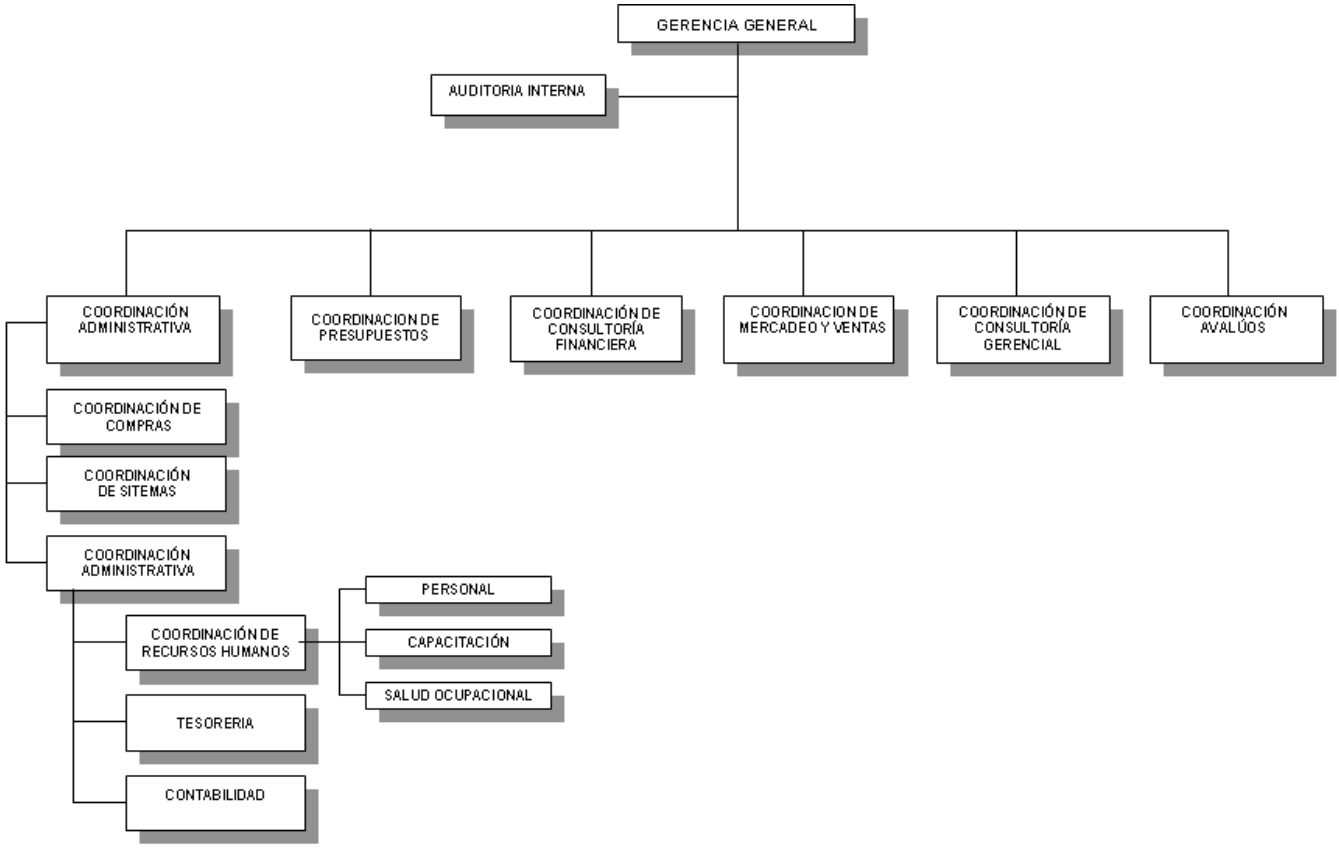

Gráfico 9: Organigrama
Fuente: La Entidad

13.1.3.3 Misión

Ser una compañía de servicio en las áreas de consultoría, financiera, legal y puesta en marcha de proyectos de construcción y avalúo inmobiliario, que a través de un alto compromiso de su personal, de una excelente tecnología y de recursos físicos de primera calidad puede ofrecer:

- → A sus clientes proyectos plenamente satisfactorios.
- → A sus colaboradores, capacitación, participación y progreso personal y económico.
- → A sus accionistas, satisfacción, orgullo y rentabilidad.

13.1.3.4 Visión

Ser en el año 2010 la compañía más competitiva del sector para lograr un crecimiento real anual promedio del 20% en horas/hombre. Estar en condiciones de ser selectivos en la contratación de trabajos y ser la primera en la mente de nuestros clientes.

13.1.3.5 Objetivos

- → Aumentar la presencia en el mercado centroamericano en un 40%.
- → Satisfacer las necesidades de los clientes logrando una calificación mínima de 7 en el desarrollo de nuestra gestión.
- → Obtener como resultado de un promedio de los servicios ejecutados, una utilidad del 16% en servicio sobre venta.
- → Asegurar la capacitación, entrenamiento y desarrollo de los colaboradores en las herramientas, principios y competencias que son fundamento y apoyo de los servicios de calidad que brinda la compañía.

13.1.3.6 Valores y ética

Es de vital importancia para la organización generar un ambiente ético de trabajo que les garantice la permanencia en el mercado a largo plazo. Es consciente de que la ética fomenta el desarrollo personal y por ende el económico.

Estos valores se apoyan en el manual de convivencia que surgió de la preocupación permanente por el desarrollo del talento humano, que redunda en el mejoramiento continuo del ambiente de trabajo.

- → Honestidad.
- → Profesionalismo.
- → Actitud de servicio.
- → Respeto a los colaboradores.
- → Actitud de aprendizaje.
- → Disposición al cambio.
- → Lealtad.
- → Sentido de pertenencia.

13.1.3.7 Servicios

Los servicios que ofrece la organización incluyen:

- → Formulación de proyectos de construcción.
- → Análisis de estructuras.
- → Avalúos inmobiliarios.
- → Alquiler de equipo de construcción.
- → Gerencia de construcciones.
- → Control financiero de construcciones.
- → Proyectos de llave en mano.

→ Tramites municipales de construcción.

13.1.3.8 Procesos de negocio

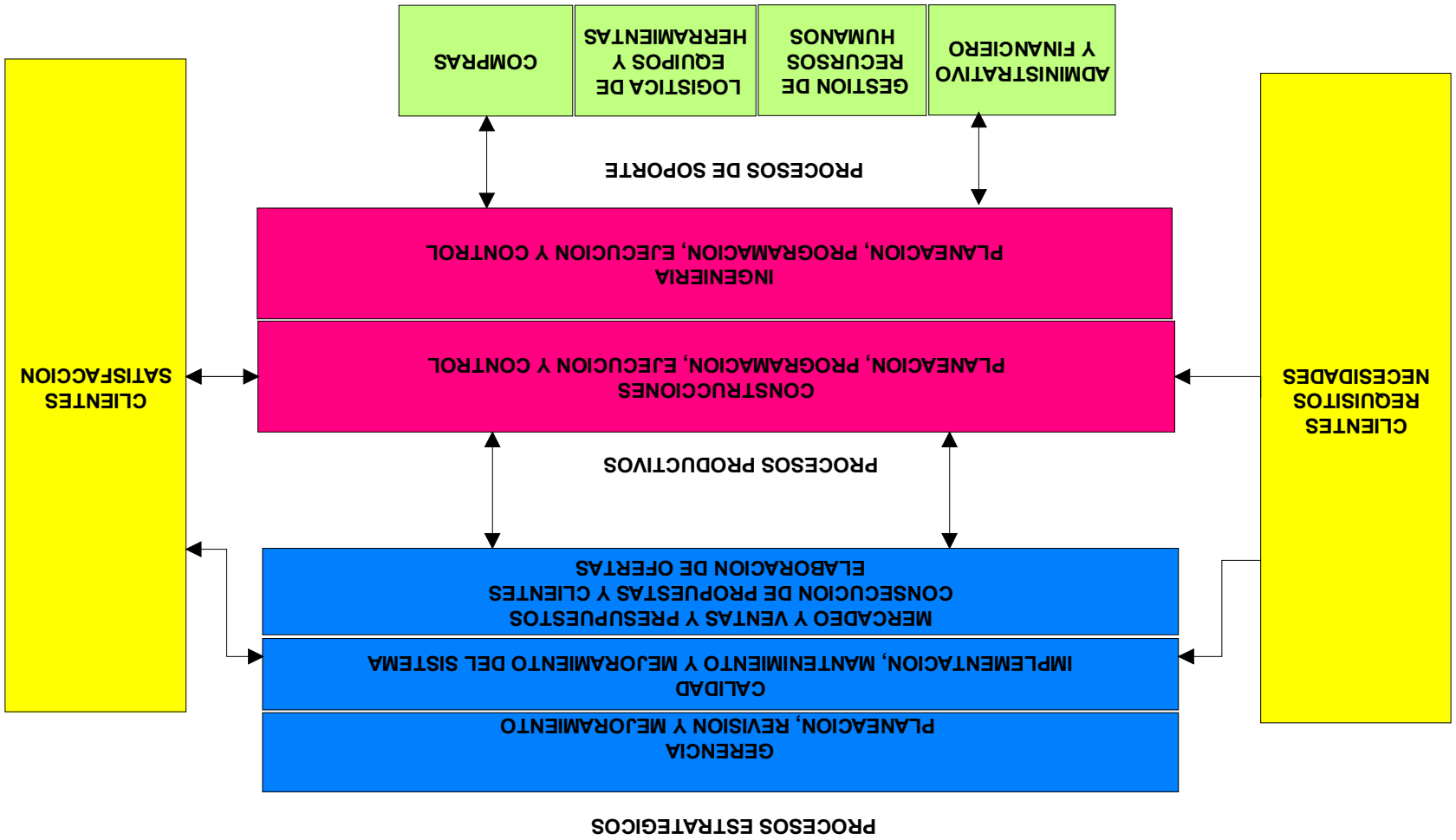

Gráfico 10: Procesos de Negocio
Fuente: La Entidad

13.1.3.9 Administración y Planificación del Área de TI

La entidad no posee una figura de comité de tecnologías, los temas relacionados a tecnología se tratan en el Comité Ejecutivo. Esta comisión se encarga de definir las estrategias y dar seguimiento a nivel macro de la ejecución de dichas estrategias. Las reuniones del Comité Ejecutivo quedan documentadas en las actas.

El Comité Ejecutivo está compuesto por la gerencia general y los coordinadores de área.

El Coordinador Administrativo desarrolla un plan de acción orientado a alcanzar los objetivos fijados por el Comité Ejecutivo. Este plan define los proyectos que cada área debe realizar, en caso de requerir procesos tecnológicos, se le informa a tecnología para que éste presupueste el tiempo y recursos económicos.

Los planes estratégicos son definidos a cinco años y los planes de trabajo desarrollados por Negocios se realizan anualmente y estos se definen en:

- → Clientes.
- → Ingresos.
- → Negocios.
- → Soporte y herramientas técnicas.

Tecnología no define un presupuesto anual para el área, si no, por cada proyecto definido en el plan de trabajo anual, se realiza un presupuesto dos o tres meses antes de iniciar el proyecto, esto se conoce en la institución como presupuesto base 0.
Debido a que el Comité Ejecutivo ha aprobado las estrategias y proyectos a ejecutar para alcanzarlas, no se requiere de una probación de ese Comité para

todos los presupuestos de Tecnología. En vez de ello, se ha definido una escala de autorizaciones por montos de inversión, donde dependiendo del monto del presupuesto, pasa por un flujo de aprobaciones.

13.1.3.10 Adquisiciones y proveedores

El proceso de selección de nuevos proveedores inicia cunado un usuario presenta un requerimiento Tecnología, quien analiza el requerimiento e identifica si es necesaria la contratación de un proveedor para el desarrollo del requerimiento o si el personal interno dispone de los recursos. En caso de contratar a un proveedor externo se buscan las opciones disponibles en el mercado y se selecciona el que cumpla con:

- → Cumplimiento de característica o requerimientos
- → Se apegue a los estándares de la Entidad
- → Experiencia en el campo
- → Presencia en el país
- → Cliente maduro en el mercado o región
- → Relación de los nuevos proveedores con los proveedores actuales
- → Precio

La aprobación de la compra se realiza según el monto y está definido por medio de una escala en la política de compras.

13.1.3.11 Seguridad

Actualmente no ha definido una política de seguridad que en conjunto dé directrices, normas, procedimientos e instrucciones, guíe las actuaciones de trabajo y defina los criterios de seguridad para que sean adoptados a nivel local o institucional, con el objetivo de estandarizar y normalizar la seguridad tanto en el ámbito humano como en el tecnológico.

Sin embargo, sí han documentado algunas políticas relacionadas con la seguridad como es el caso de:

- → Uso de Internet
- → Uso de Correo Electrónico
- → Política de administración de equipo tecnológico

En las cuales se define que la responsabilidad del uso de los recursos es del usuario debido a que a éste se le hace entrega de un equipo con usuario y contraseña para su uso personal.

Estas políticas aplican a todo el personal que haga uso de los recursos tecnológicos.

Los métodos de control de acceso lógico son contraseñas que define el usuario final y pueden ser utilizadas más de una vez.

Para que a un usuario final se le otorguen privilegios de acceso sobre las aplicaciones, se le crea un perfil de usuario y se le remuevan o inactivan los accesos. Debe existir un correo electrónico del jefe inmediato solicitando o eliminado los accesos.

Como mecanismos de seguridad física y ambiental, se poseen las siguientes medidas:

- → Llavines tradicionales de control de acceso a la sala de servidores.
- → Una bitácora de visitantes que posee el guarda de seguridad a la entrada de las instalaciones.
- → Aire acondicionado.
- → Extintores de fuego.

13.1.3.12 Hardware, Redes Y Comunicaciones

La entidad posee una red LAN de cuarenta estaciones de trabajo, siete servidores, dos enrutadores y un firewal.

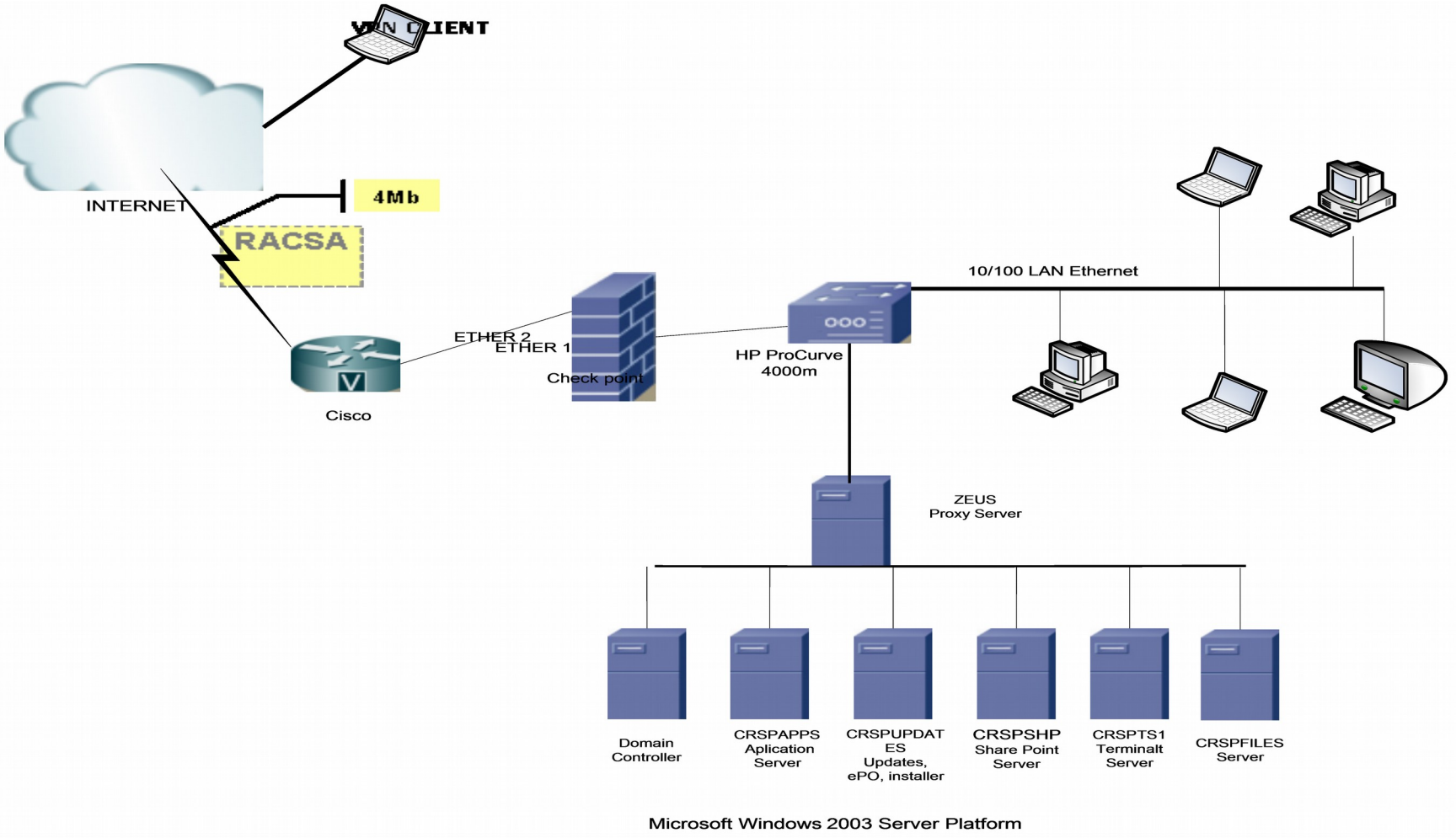

Gráfico 11: Diagrama LAN
Fuente: La Entidad

Por medio de los enrutadores y el firewall se conectan de manera remota por VPN funcionarios de la entidad. Esta conexión es requerida para el registro de horas laboradas, acceso a las unidades compartidas y en ocasiones comunicaciones por voz cuando el funcionario está fuera del territorio nacional.

Existe un proyecto para implementar enlaces VPN permanentes con Nicaragua y El Salvador.

13.1.3.13 Continuidad de las Operaciones

Consultores Asociados S.A. está en proceso de desarrollar un plan de continuidad de negocio, que incluye como un apartado las contingencias tecnológicas. Este plan será desarrollado por una empresa consultora, cuya fase del proyecto es actualmente la negociación de los honorarios. Una vez aprobada esta fase se iniciará con el desarrollo.
Se identificó que los mecanismos contingentes implementados son:

- → Equipos UPS que brindan energía a los servidores y estaciones de trabajo por períodos de 30 minutos en caso de fallas en el fluido eléctrico.
- → Respaldos de las bases de datos.
- → Replicación de las bases de datos cada 30 minutos en servidores separados.

13.1.3.14 Mantenimiento e implementación de Sistemas de Información

Los sistemas de aplicación fueron adquiridos a una empresa externa reconocida en el mercado Costarricense, suyo software ofrece una solución para todos los procesos financieros contables del negocio. Antes de implementar el sistema contable, la contabilidad era llevada en outsourcing. Esta empresa utilizaba el software QuickBooks para el control contable de La Entidad. Cuando La Entidad

eliminó el outsourcing porque su operación estaba creciendo y prefirió ejecutar este proceso internamente, se decidió adquirir una aplicación contable y es donde por medio de un proceso de selección de tres diferentes paquetes de software, incluyendo QuickBooks. Después de realizado el proceso fue necesario ejecutar procesos pruebas de la aplicación, aprobación de las pruebas y migración o conversión de datos.

Esta implementación se realizó en agosto del 2003.

A continuación se presenta un diagrama de los módulos de software implementados en la firma Consultores Asociados S.A.:

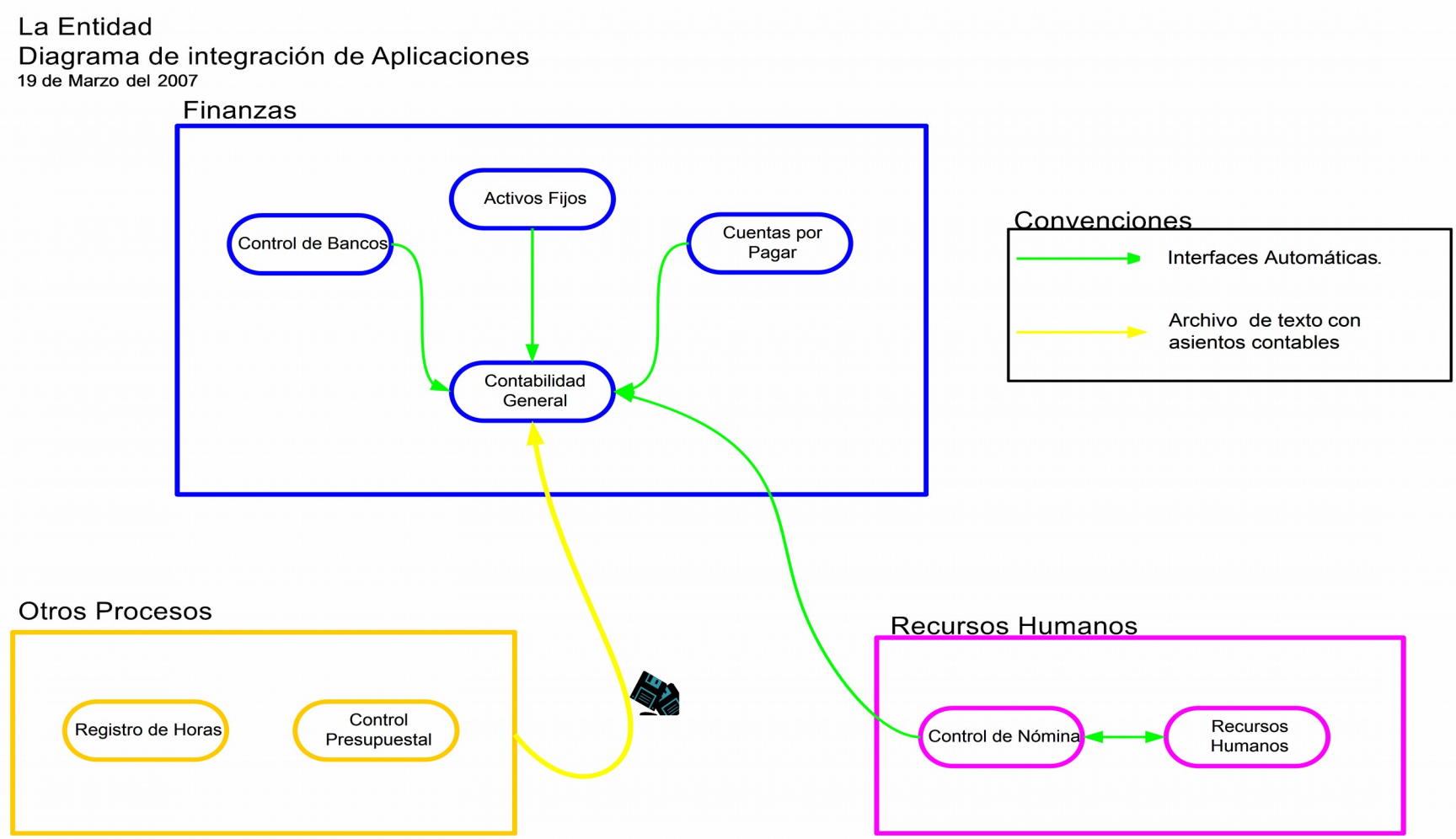

Gráfico 12: Integración de Aplicaciones
Fuente: Desarrollo propio

13.1.3.15 Software y Bases de Datos

Como estándar de trabajo para las bases de datos y sistemas operativos se utilizan los productos Microsoft. Todos los sistemas y configuraciones existentes son administrados por el personal interno de la Entidad.

Las bases de datos poseen configurados trabajos automáticos para la identificación de bloqueos en los registros y realización de ajustes al rendimiento de la misma. Los sistemas operativos no poseen configuraciones adicionales de seguridad, como un hardening y tampoco existe un estándar de configuraciones que permita identificar los componentes necesarios según los servicios a desempeñar por el sistema operativo y como éstos deben estar configurados.

13.1.4 Evaluación de riesgos

Para el proceso de evaluación de riesgos se partió de los objetivos del negocio y componentes de tecnología que están colaborando en la consecución de dichos objetivos.

Objetivo de Negocio	Activos TI
Aumentar la presencia en el mercado centroamericano en un 40%.	* Centrales telefónicas IP. * Portal de Internet. * Administración de conocimiento e información. * Equipos de cómputo personales. * Telecomunicaciones.
Satisfacer las necesidades de los clientes logrando una calificación mínima de 7 en el desarrollo de nuestra gestión.	* Herramientas de software de consultoría y avalúo. * Correo electrónico.
Obtener durante como resultado de un promedio de los servicios ejecutados, una utilidad del 16% en servicio sobre venta.	* Maximización del uso de las tecnologías de procesamiento y telecomunicaciones. * Sistema de control de horas y gastos. * Sistema contable. * Sistema de facturación. * Sistema de Cuentas x Cobrar. * Sistema de Cuentas x Pagar.
Asegurar la capacitación, entrenamiento y desarrollo de los colaboradores en las herramientas, principios y competencias que son fundamento y apoyo de los servicios de calidad que brinda la compañía.	* Portal de capacitación y conocimiento. * Conocimiento personal de tecnología.

Tabla 5: Objetivos de Negocio Vrs Activos de TI

Identificados los activos de tecnología versus los objetivos, se procedió a invitar a funcionarios clave de la entidad para aplicar un proceso de identificación de amenazas que enfrenta los activos de Tecnología y definición de cuáles vulnerabilidades posee la organización ante dichas amenazas. Los funcionarios clave que participaron fueron:

→ Coordinador Administrativo.

→ Presupuestos.

→ Consultoría Financiera.

→ Ventas.

→ Consultoría Gerencial.

→ Avalúos.

→ Contador General.

→ Auditor Interno.

→ Recursos Humanos.

→ Coordinación de sistemas.

El resultado de la identificación de amenaza, vulnerabilidades y los riesgos que enfrenta la entidad es:

Amenaza	Vulnerabilidad	Riesgo
* Accesos no autorizados. * Espionaje industrial. * Sabotaje. * Falla eléctrica. * Ataques de hacking a los equipos. * Virus.	* Usuarios con accesos que no le corresponden. * Débiles políticas de contraseña. * Inexistencia de procesos de autenticación con 3 factores. * Información importante no codificada. * Inexistencia de mecanismos de generación alterna de energía. * Acceso libre a los equipos de comunicación y procesamiento. * Inexistencia de firewall y detectores de intrusos.	* Robo de información. * Robo de equipos personales. * Fuga de información. * Destrucción de información. * Pérdida de información por fallas. * Falla en la disponibilidad de los servicios de comunicación y procesamiento. * Equipos quemados por sobre voltajes. * Pérdidas económicas. * Imagen empresarial decaída.
* Espionaje industrial. * Virus corrompa la base de datos. * Intercepción de correos electrónicos.	* Débil procedimiento de respaldos de información. * Antivirus no actualizado. * Información confidencial no codificada.	* Fuga de software clave desarrollado internamente. * Divulgación de información confidencial. * Pérdida de clientes. * Imagen empresarial decaída.

* Modificación no autorizada de los datos. * Pérdida de información. * Accesos no autorizados. * Falla en la disponibilidad de los sistemas por entes naturales o ambientales.	* Incorrecto otorgamiento de privilegios. * Usuarios de ex empleados no eliminados. * Inexistencia de registros (bitácoras) de modificaciones a información significativa o importante.	* Existencia de registros no autorizados. * Modificación de cifras contables.
* Rotación de personal por nuevas transnacionales de tecnología. * Obsolescencia de conocimiento.	* No poseer programas de educación continua. * No incentivar al empleado. * No administrar el conocimiento que posee el empleado, documentado procedimientos. * No poseer un sistema de registro de problemas para dar futuras soluciones. * No poseer documentación sobre las configuraciones de los sistemas de procesamiento y comunicación.	* Sistemas que no pueden ser administrados fácilmente. * Dependencia del personal de tecnología.

Tabla 6: Amenazas, Vulnerabilidades y Riesgos

		Calificación		
ID	**Riesgos**	**Vulnerabilidad**	**Impacto**	**Valor de Riesgo**
1	Fuga de software clave desarrollado internamente.	0.2	10	**2**
2	Existencia de registros no autorizados.	0.2	40	**8**
3	Sistemas que no pueden ser administrados fácilmente.	0.6	10	**6**
4	Equipos quemados por sobre voltajes.	0.2	80	**16**
5	Modificación de cifras contables.	0.2	80	**16**
6	Pérdida de clientes.	0.2	100	**20**
7	Destrucción de información.	0.4	60	**24**
8	Fuga de información.	0.6	40	**24**
9	Divulgación de información confidencial o Robo de información	0.6	60	**36**
10	Falla en la disponibilidad de los servicios de comunicación y procesamiento.	1	40	**40**
11	Imagen empresarial decaída.	0.4	100	**40**
12	Pérdidas económicas.	0.6	100	**60**
13	Pérdida de información por fallas.	0.8	80	**64**
14	Dependencia del personal de tecnología.	0.8	100	**80**
15	Robo de equipos personales.	1	80	**80**
16	Robo de información.	1	80	**80**

Tabla 7: Vulnerabilidad, Impacto y Riesgo

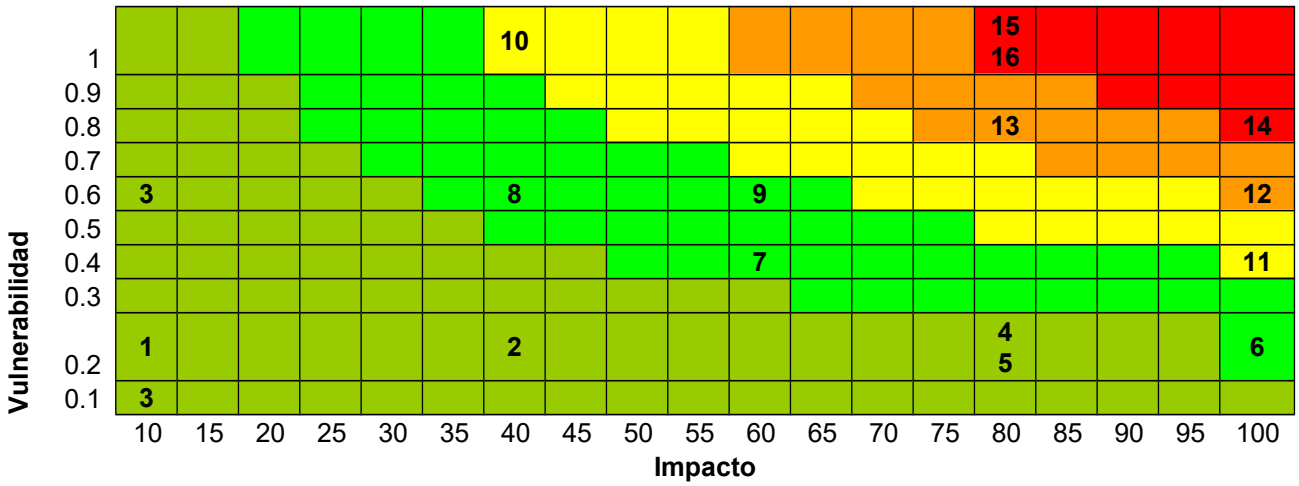

Gráfico 13: Mapa de Riesgos
Fuente: Desarrollo propio

13.1.5 Programa de auditoría

Con base en la evaluación de riesgos realizada se definió que los objetivos de auditoría se dividirían en tres áreas:

- → Control de Acceso
- → Seguridad Física y Ambiental
- → Continuidad del Negocio

Estos objetivos de auditoría están alineados con el estándar ISO-17799.

13.1.5.1 Control de Acceso

Dentro de la estructura de la organización se deberá comprobar si existe una función para la administración y control de la seguridad de acceso a los datos, un responsable de seguridad que sea independiente del área de Sistemas de Información y que se reporte al máximo nivel de autoridad.
Debe observar si existe una política formal de seguridad informática, en la que se detallen como mínimo los siguientes aspectos: nivel de confidencialidad de los datos, procedimiento de otorgamiento de claves de usuarios para el ingreso a los sistemas, y estándares fijados para el acceso de usuarios.
El revisor debe determinar si las claves son personales y secretas. Debe verificar la existencia de un procedimiento de inhabilitación automática de claves de usuarios que no hagan uso de la misma por un período predeterminado y si existe un procedimiento formal para la baja de usuarios que dejen de pertenecer a un departamento o a la organización.
El revisor verificará que el sistema de seguridad mantenga los archivos de claves o "passwords" encriptadas , generar reportes de auditoría sobre intentos de violaciones, el uso de utilitarios sensitivos y las actividades de los usuarios con atributos de administración y accesos especiales, los que deberán mantenerse en archivo durante el tiempo que fijan las normas para cada caso,

utilizando para ello soportes de almacenamiento (papel, CD, disco óptico u otras tecnologías de esa características).

Debe verificar la existencia de una adecuada planificación y documentación escrita y actualizada de las actividades que se desarrollan normalmente en el centro de procesamiento de información, que deberá incluir como mínimo el detalle de los procesos a realizar, los controles que se efectúan, los mecanismos de registro de los procesos y sus problemas, los procedimientos sobre cancelaciones y reproceso, las relaciones con otras áreas y los mecanismos de distribución de información.

Debe constatarse de la existencia de procedimientos de control para garantizar la efectividad de cambios cuando corresponda, tales como: cambios de programas en bibliotecas de producción, en los archivos, cambios en las definiciones de diccionarios de datos, en las órdenes de corrida de programas, etc.

En los casos en que existan distintos centros de procesamiento debe considerar si existen responsables del control centralizado de las operaciones y procesos que se realicen en cada uno de ellos.

Debe verificar, si es necesario con pruebas, que los sistemas de información computarizados tengan incorporados en su aplicación, validaciones y controles mínimos para asegurar la integridad y validez de la información que procesan. Deben existir procedimientos de control formales que aseguren la integridad de la información que se ingresa y procesa en los sistemas.

Debe comprobar que se dispone de equipamiento alternativo (propio o por convenios formales con terceros) para el procesamiento y las telecomunicaciones, a efectos de poder superar posibles fallas o interrupciones de las actividades en sus equipos habituales. Deberá estar localizado en un edificio ubicado a una distancia razonable del centro de procesamiento.

Los objetivos de auditoría para el área de control de acceso son:

- → Verificar que la empresa considere los controles adecuados para que el acceso a la información y los procesos de negocio se brinden sobre la base de los requerimientos, la seguridad y del negocio.
- → Verificar la definición y documentación de los requerimientos de negocio para el control de accesos.
- → Verificar que las reglas y derechos del control de accesos, para cada usuario o grupo de usuarios, sean claramente establecidos en una declaración de política de accesos.
- → Verificar que los usuarios y proveedores de servicio cuenten una clara enunciación de los requerimientos comerciales que deberán satisfacer en términos de controles de acceso

13.1.5.2 Seguridad Física y Ambiental

La seguridad física es un factor de suma importancia en los centros de cómputo instalado o a instalar. Esta consideración se refleja en la elección de las normas a considerar para la ubicación del procesador, materiales utilizados para su construcción, equipo de detectores y protección contra incendios, sistema de aire acondicionado, instalación eléctrica, sistema de control de acceso y el entrenamiento al personal u operadores.

Durante la evaluación, se tratará la seguridad física como un conjunto integrado de capacidades y soluciones que deben proveerse en una empresa o centro de computación para mantener la seguridad en un nivel aceptable, intentando ir de lo global a lo específico. Desde el edificio donde se alojará el hardware y el suministro de energía o el control de accesos hasta lo más específico del hardware que ha de soportar las aplicaciones.
Es muy importante ser consciente que por más que la empresa sea la más segura desde el punto de vista de ataques externos (hackers, virus, ataques de DoS, etc.); la seguridad de la misma será nula si no se ha previsto como

combatir un incendio o cualquier otro tipo de desastre natural y no tener presente políticas claras de recuperación.

La seguridad física es uno de los aspectos más olvidados a la hora del diseño de un sistema informático. Si bien algunos de los aspectos de seguridad física básicos se prevén, otros, como la detección de un atacante interno a la empresa que intenta acceder físicamente a una sala de cómputo de la misma, no. Esto puede derivar en que para un atacante sea más fácil lograr tomar y copiar una cinta de "backup" de la sala de cómputo, que intentar acceder vía lógica a la misma.

Así, la Seguridad Física 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". Se refiere a los controles y mecanismos de seguridad dentro y alrededor del centro de cómputo, así como los medios de acceso remoto al y desde el mismo; implementados para proteger el hardware y medios de almacenamiento de datos.

El auditor deberá revisar detalladamente los controles de:

- → Situación del área del centro de cómputo.
- → Almacenamiento de la información.
- → Equipos contra incendios.
- → Suministro de energía eléctrica.
- → Seguridad en el acceso del personal en áreas restringidas.
- → Preparación para desastres naturales, incendios accidentales, tormentas e inundaciones.
- → Preparación contra amenazas ocasionadas por el hombre como disturbios, sabotajes internos y externos deliberados.

Los objetivos de auditoría para el área de Seguridad Física y Ambiental son los siguientes:

→ Verificar el tratamiento de la empresa para impedir accesos no autorizados, daños e interferencia a las sedes e información de la empresa.

→ Verificar la ubicación de las instalaciones de procesamiento de información crítica o sensible de la empresa y que los controles de seguridad física estén alineados con las mejores prácticas.

13.1.5.3 Continuidad del Negocio

Los clientes esperan que las compañías estén disponibles en todo momento, 24 horas al día y 7 días a la semana. Por lo tanto, la continua disponibilidad operacional es un propulsor de negocios muy importante en la actualidad. La capacidad de mantener una compañía en funcionamiento, a pesar de pequeñas o grandes interrupciones, es simplemente una manera de brindar servicio a los clientes y los mercados, al tiempo que se mantiene la competitividad. Las empresas que tienen planes de continuidad de negocio y de recuperación frente a siniestros son las que esperan mantenerse en el negocio por mucho tiempo. En cambio, las compañías que no los poseen, están dejándolo al azar y los clientes y accionistas son los que asumen los riesgos.

En los planes de continuidad de negocio se trata de analizar por completo la empresa, el impacto total en costos, asociados con una interrupción de sus actividades comerciales diarias. Si bien un plan de continuidad de negocio completo suele ir más allá de la infraestructura de TI y se inserta dentro de un vasto plan de reanudación de actividades que involucra personas, procesos y productos, para el presente trabajo se delimitará en el área de TI.

Un plan sólido de continuidad de negocio intenta “hacer las cosas bien”. De la misma manera que se tienen planes de seguros, tener un plan de continuidad de negocio es prueba de que la empresa ha planificado la supervivencia económica de los inversionistas, clientes y empleados en caso de cualquier contingencia. En pocas palabras, es una buena política corporativa. Y aunque el plan de

continuidad del negocio es una necesidad dentro del ambiente empresarial altamente interconectado de nuestros días, no es un concepto nuevo. En algunos mercados esta práctica ya tiene años, pero hoy es un requerimiento común dentro de muchas empresas y una forma de decirle al mercado que usted estará allí cuando lo necesiten.

Los objetivos de auditoría para el área de Continuidad del Negocio son:

- → Verificar el establecimiento de controles para contrarrestar las interrupciones de las actividades comerciales y proteger los procesos críticos de los negocios de los efectos de fallas significativas o desastres.
- → Verificar la implementación de un proceso de administración de la continuidad de los negocios para reducir la discontinuidad ocasionada por desastres y fallas de seguridad (que pueden ser el resultado de, por ej., desastres naturales, accidentes, fallas en el equipamiento, y acciones deliberadas) a un nivel aceptables mediante una combinación de controles preventivos y de recuperación.
- → Verificar que sean analizadas las consecuencias de desastres, fallas de seguridad e interrupciones del servicio.
- → Verificar la existencia e implementación de planes de contingencia para garantizar que los procesos de negocios puedan restablecerse dentro de los plazos requeridos.
- → Verificar que la administración de la continuidad de los negocios incluya controles destinados a identificar y reducir riesgos, atenuar las consecuencias de los incidentes perjudiciales y asegurar la reanudación oportuna de las operaciones indispensables.

13.2 Evaluación del control

13.2.1 Medir la suficiencia y validez de los controles existentes

En el estudio se utilizaron tres técnicas para recolección de pruebas y evidencias sobre la seguridad de los sistemas informáticos: entrevistas, cuestionarios y Herramientas TAACS de Seguridad.

13.2.1.1 Entrevistas

Las entrevistas se han utilizado para obtener información tanto cualitativa como cuantitativa. Su objetivo fue lograr respuestas francas, completas y honestas de un entrevistado que tiene más información sobre el tema de la entrevista que el propio auditor. Se ha pretendido que las entrevistas no sean un interrogatorio, en el sentido de que no se ha planteado de antemano ningún tipo de antagonismo entre el entrevistador (el auditor) y el entrevistado. Las entrevistas constaron de tres fases principales:

- → La preparación de la entrevista.
- → La realización de la entrevista.
- → El análisis de la entrevista ya realizada.

Las entrevistas se han utilizado para encontrar información relevante de primera mano dada la limitación de tiempo con que se ha contado para el estudio.

13.2.1.2 Cuestionarios y guías de auditoría

Los cuestionarios y guías de auditoría han sido mayormente construidos basados en la Norma ISO 17799. Para este trabajo se ha considerado dentro de los cuestionarios la necesidad de que el consultor obtenga datos relevantes por medio de los cuestionarios.

Los cuestionarios y guías utilizados han colaborado directamente en la realización de la auditoría y se ha determinado que deben incluir los siguientes principios básicos:

1. Necesidad de preparación del cuestionario y guía con anterioridad a la aplicación.
2. Necesidad de alinear el cuestionario con el sistema de control interno de la organización auditada.
3. Actitud mental independiente en el proceso de diseño.
4. Debe ser suficientemente completos para brindar una adecuada evidencia del trabajo realizado y ser soporte documental de las conclusiones alcanzadas.

13.2.1.3 Herramientas

Los ambientes de las empresas son muy complejos, y las vulnerabilidades de la seguridad son numerosas. Los sistemas se deben comprobar sobre una base regular para asegurarse de que estén en conformidad con los mejores estándares de la práctica. Los servidores se deben comprobar para asegurarse que tengan ciertos ajustes de seguridad y los parches apropiados. Para la mayoría de los procesos de revisión, la comprobación manual al nivel del detalle requerido no es factible. Es virtualmente imposible dar un criterio completo sin tener un “set” de herramientas apropiadas para automatizar algunas de estas funciones de la revisión de seguridad.

Algunas de las áreas donde se han utilizado herramientas en este proceso incluyen:

→ Análisis de vulnerabilidades para la infraestructura.

→ Comprobar la corrección de vulnerabilidades

→ Análisis de vulnerabilidad de contraseñas

→ Análisis de vulnerabilidades en sistemas Microsoft

Se considera que una herramienta adecuada para el análisis de vulnerabilidades debe cumplir con los siguientes criterios avalados por el NIST:

- → Precisión, fácil de usar, administración y “overhead” son factores que deben considerarse en la selección.
- → Esquema de operación que opere bajo la modalidad “de afuera hacia adentro” como un “hacker”, desde la perspectiva de un tercero.
- → Asegurar resultados precisos sobre dispositivos de red, puertos, protocolos y sistemas sin hacer ningún tipo de presunciones.
- → Empleo de un eficiente esquema de inferencia para la evaluación.
- → Escaneo automático que utilice bases de datos actualizadas constantemente sobre métodos de ataques y vulnerabilidades.
- → La herramienta (servicio) debe minimizar caídas o fallas de servidores, ciclos y otros problemas causados de manera inadvertida por las actividades de escaneo.
- → La solución debe proveer opciones de escaneo preferenciales como intensidad, velocidad de tal forma que no haya sobrecarga sobre redes, servidores y “scanners” como tal.
- → Las actualizaciones sobre vulnerabilidades de las bases de datos del producto ofrecido debe poderse realizar desde localidades remotas bajo demanda o de manera automática.
- → Deben proveerse medidas de remediación para la mitigación de cada vulnerabilidad encontrada y proveer referencias a información adicional.
- → Deben reportarse el número CVE para cada vulnerabilidad encontrada.
- → Generación de reportes concisos, ajustables que incluyan priorización de vulnerabilidades por severidad y análisis de tendencias, además, de permitir la comparación con resultados previos.

13.2.2 Identificar áreas débiles o vulnerables.

Para la evaluación de la seguridad se utilizó la herramienta Internet Scanner de IBM por ser una herramienta probada en los laboratorios de West Coast Labs[14] donde se identificó que esta herramienta detecta el 100% de las vulnerabilidades críticas y el 90% de las vulnerabilidades serias. Adicional se utilizó al herramienta Microsoft Baseline Security Analyzer 2.1, que nos permitió identificar el nivel de actualices de seguridad implementadas en los servidores y bases de datos SQL Server.

Adicional a estas dos herramientas se aplicaron las guías de auditoría descritas en el punto 13.1.5 Programa de Auditoría por medio de los métodos indicados en el punto 13.2.1.

13.3 Comunicación de resultados

13.3.1 Preparación de recomendaciones

De acuerdo con las recomendaciones presentadas en el informe, es prioritario que Consultores Asociados inicie un proceso de creación de una organización de seguridad bien estructurada. La creación de esta organización es fundamental dentro de cualquier programa de seguridad y necesita establecerse antes de que surja cualquier cambio mayor en la infraestructura de seguridad de la organización.

Se recomienda que esta organización sea independiente del departamento de Tecnología de Información (IT) y reportar al nivel más alto de gerencia. Este es un requisito que a menudo se pasa por alto en las organizaciones; pero es crítico para que la organización tenga éxito al implantar políticas y los cambios técnicos para toda la compañía. Además, este grupo define los papeles y las responsabilidades del equipo de seguridad y funge como el comité responsable de la seguridad de información.

[14] Información obtenida del sitio Web del fabricante, http://www.iss.net/products/Internet_Scanner/product_main_page.html

Debe existir un sub-comité de esta organización, el cual poseerá la autoridad de administrar las políticas. Este grupo será responsable de la creación, implantación y aplicación de las políticas de seguridad dentro de la compañía y también de cualquier política especializada y relacionada con seguridad informática. Adicionalmente, este grupo debe establecerse con el fin de alcanzar un consenso en el conjunto de políticas de seguridad aplicables a toda la compañía. El subcomité de administración de políticas debe ser creado para asegurar consenso entre los documentos corporativos y las políticas, con el fin de proporcionar la ayuda requerida para la implantación y aplicación de las mismas.

Una vez que este grupo haya sido conformado y se encuentre en ejecución, se debe completar la implantación de las políticas aprobadas para el desarrollo de un estándar para la protección de información. Estos documentos, son la columna vertebral y funcional para la arquitectura de seguridad que se debe crear. Además, los mismos deben ser flexibles y adaptables a las necesidades y cambios del negocio. La autoridad encargada de la administración de políticas debe también coordinar con departamentos técnicos para crear los estándares que serán utilizados por los departamentos para hacer cumplir los estatutos documentados en cuanto a política se refiere. Estos controles técnicos aseguran que los niveles de seguridad mínimos se estén manteniendo dentro de la organización.

Existen varias vulnerabilidades y problemas asociadas a la arquitectura actual del cliente. Actualmente no existe redundancia en muchos de los sectores críticos de la red. Por ejemplo, se encontró un switch el cual si falla o es víctima de un ataque de negación de servicios, hará que se pierdan todas las comunicaciones externas.
Adicionalmente se recomienda instalar herramientas de monitoreo en todos los puntos posibles de la red que comunica y la conexión remota, ya que esto ayuda a identificar anomalías en el uso de los servicios.

Actualmente el cliente no posee un sistema de control de acceso a la red interna que garantice la seguridad en caso de haberse comprometido la seguridad de alguna de las conexiones. Se deben desarrollar métodos de control de acceso que proporcionen una mayor seguridad y confiabilidad

A medida que se desarrollaba el programa de auditoría se identificaron áreas de mejora que fueron documentadas en el formato Anexo 1.7 C-1-1 Formato Recomendaciones. Las recomendaciones plasmadas en el formato C-1-1 fueron discutidas con el encargado del proceso tan pronto como se identificaron para validar la razonabilidad de la misma e identificar si existían controles compensatorios.

A continuación se presentan un gráfico de resumen donde se observa el total de observaciones identificadas y su importancia.

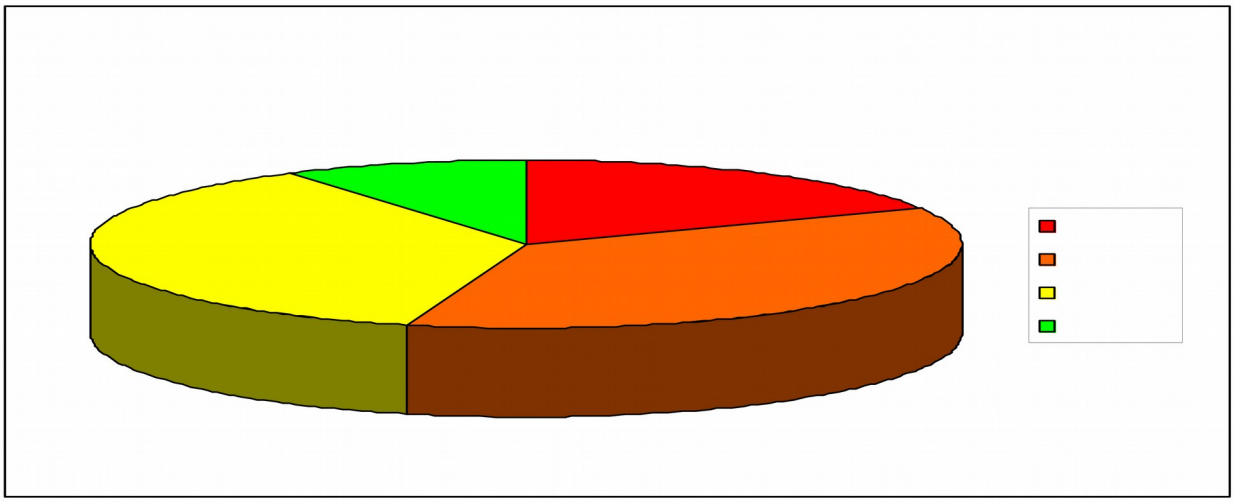

Gráfico 14: Gráfico de Observaciones
Fuente: Desarrollo propio

A manera de ejemplo se incluyen dos recomendaciones de las cuales la administración de la Entidad estuvo de acuerdo en publicar:

14 Configuración de parámetros de contraseñas

Condición:
Actualmente la Entidad posee dos niveles de seguridad para el acceso a los sistemas, el primer nivel es el acceso al sistema operativo, aquí no se han configurado parámetros de contraseñas referentes al histórico de contraseñas, contraseñas complejas, Intentos de acceso fallidos, duración del la inactivación de la cuenta después del bloqueo y mínimo de caracteres en la contraseña, el segundo nivel está ubicado en el sistema Financiero Contable, donde se comprobó que 10 usuarios no poseen configurado el parámetro de seguridad de vencimientos periódicos de contraseñas.

Criterio:
El estándar de seguridad ISO 17799-2005 indica en el punto 11.5.1 que un proceso de ingreso seguro debe registrar los intentos de acceso fallidos realizados por el usuario y almacenar la cantidad de intentos realizados, la fecha y hora en que fueron realizados y bloquear la cuenta del usuario después de que se alcance el total de intentos fallidos. Adicionalmente el punto 11.5.3 describe los parámetros de contraseña para utilizar contraseñas de calidad. Los parámetros incluidos en el estándar son:

0. Cambio periódico de la contraseña.
1. Poseer un histórico de contraseñas para prevenir su uso.
2. No desplegar las contraseñas mientras son digitadas.
3. Almacenar y transmitir las contraseñas de forma encriptada.
4. Contraseñas complejas, es decir, que incluyan números, letra y caracteres especiales.

Causa:
La Entidad no ha definido las políticas de contraseña debido a que los usuarios finales se quejan de lo complejo que es para ellos utilizar contraseñas de composición compleja y lo difícil de recordarlas.

Efecto:

El no poseer implementados parámetros de contraseñas podría ocasionar que ante un ataque de diccionario sea más fácil o simple para el atacante identificar una contraseña trivial o débil, además el no obligar a los usuarios finales a realzar el cambio de la contraseña haría posible que esta a través del tiempo sea conocida por personal cercano a la usuario y este haga uso no autorizado, afectando los criterios de integridad, confidencialidad de la información.

Recomendación:
Crear una política que defina el uso de las contraseñas en la organización y configurar los siguientes parámetros de seguridad de contraseñas para los sistemas tecnológicos de la Compañía:

Sistema operativo:

- → Recordad las 6 últimas Historial de contraseñas.
- → Uso de contraseñas complejas.
- → Tres Intentos de acceso fallidos.
- → Bloqueo de la cuenta por 30 minutos.
- → Mínimo seis caracteres en la contraseña.

Sistema de Aplicación:

- → Vencimientos periódicos de contraseñas entre 30 y 90 días.

Comentario de la Gerencia:
Observación acepta y se procederá a su implementación.

2. Procedimiento de validación de accesos otorgados

Condición:
La Compañía no ha establecido un procedimiento para que los usuarios responsables de sistemas reciban periódicamente el detalle de los accesos otorgados con el fin de verificar su vigencia, validez, aplicación y el nivel de

segregación existente en relación a las actividades realizadas por los funcionarios a su cargo.

Criterio:
El estándar de seguridad ISO 17799-2005 indica en el punto 11.2.4 la necesidad de un proceso de revisión de accesos periódica y cada vez que existe un cambio en el estado del empleado.

Causa:
La administración considera que la baja rotación de sus empleados y la alta fidelidad de los mismos hacia la empresa son factores que minimizan o eliminan el riesgo de que un usuario haga un incorrecto uso de los accesos asignados en pro de un bien personal.

Efecto:
La falta de revisión periódica de los accesos otorgados a los usuarios, por parte de los usuarios dueños de sistemas, incrementa el riesgo de que existan usuarios con privilegios de acceso sobre cierta información que no deberían de acceder o manipular para las funciones de las que son responsables.

Recomendación:

Elaborar, aprobar e implementar un procedimiento formal para la revisión periódica, por parte de cada responsable de sistema, de la lista de usuarios y accesos otorgados con el fin de verificar la validez y vigencia de cada uno de ellos.

Comentario de la Gerencia:
Observación acepta y se procederá a su implementación.

15 Capítulo 3: Conclusión

La aplicación de una metodología de auditoría sin duda alguna facilitó el proceso de revisión, dándole organización y concordancia entre sus fases.

Se identificó que para el auditado es importante comprender cual es trabajo que se está realizando y como encaja él en el proceso, de esta forma su participación será más activa en la auditoría.

La utilización de un marco de control conocido por la mayoría de personas o promulgado por una organización de prestigio como es la ISO, hace que las observaciones tomen un sentido de mayor importancia para la organización y sintoniza al personal administrativo y técnico en el ambiente de seguridad.

Es importante que las guías de auditoría sean desarrolladas de una forma clara y concisa, de esta forma es factible que un segundo auditor tome el proceso de revisión y no tenga que rehacer el trabajo.

La aplicación de un proceso de revisión de papeles es importante para asegurar la calidad del trabajo realizado, el cumplimiento con la metodología y para validar la evidencia soporte de las observaciones emitidas. Este proceso de revisión de calidad hará que ante una objeción en los comentarios emitidos por la auditoría, se pueda demostrar con hechos y evidencia contundente la veracidad de lo informado.

La aplicación de software para evaluación de de vulnerabilidades de seguridad permite de forma rápida identificar deficiencias, sin embargo, es de vital importancia que este software sea utilizado por personal capacitado para su uso e interpretación de resultados, pues sería posible que ante una incorrecta aplicación de la herramienta, se afecte el correcto funcionamiento de toda la

plataforma de tecnología. Situación que podría deteriorar la relación existente entre el auditor y la administración.

La formulación de recomendaciones reales y no utópicas, permite que la organización perciba el valor del proceso de auditoría.

Lecciones aprendidas

Para este proceso se ha seguido una serie de reglas básicas que han colaborado con el objetivo de una adecuada revisión de los criterios establecidos:

- → Fomentar la cooperación de los elementos auditados. Hay que convencer de que el auditor busca mejoras y soluciones, para evitar la postura defensiva y de desconfianza.
- → Contar con el apoyo de la Dirección, ya que se deberán realizar entrevistas y solicitar documentación y posiblemente trabajos de los elementos auditados.
- → Cuidar aspectos protocolarios. Explicar primero al jefe qué se desea obtener de su subordinado.
- → Realizar una presentación o entrevista inicial en la que se cuenta el objetivo, su justificación y se aclaran dudas.
- → Solicitar, con la antelación precisa, la información inicial a obtener.
- → No adelantar resultados parciales. Puede causar impresiones falsas.
- → Comentar con los interesados los resultados obtenidos, antes de presentarlos a niveles superiores.
- → En caso de que se investiguen posibles fraudes o irregularidades maliciosas, hay que cuidar que se realicen los trabajos pertinentes con el mayor sigilo posible. Y tampoco hay que comentar con los interesados los resultados obtenidos.

16 Bibliografía

16.1 Libros y Documentos

Information Systems Audit and Control Association. *Control Objectives for Information and related Technology* (COBIT®) 4.0. IT Governance Institute. 2006

International Standards Organization. "*Information technology -Security techniques -Code of practice for information security management"*, (ISO/IEC 17799:2005), 2005.

Consultores Asociados S.A., *Manual de Calidad*. Enero 2007.

Consultores Asociados S.A., *Políticas y Procedimientos*. Diciembre 2005.

Belmar, Víctor. *Prevención de riesgos - Implantación de un sistema efectivo de control del riesgo operacional en la empresa*, http://www.monografias.com/trabajos13/progper/progper.shtml

The Institute of Internal Auditor, *Definición de la auditoría interna*, http://www.theiia.org/guidance/standards-and-practices/professional-practices-framework/definition-of-internal-auditing/?search=audit%20definition

Instituto de Auditores Internos, *El Rol de la Auditoría Interna en la Gestión de Riesgo Empresarial*, año 2004.

Gentle, Chris. *Cracking the IT value code*, Deloitte 2005.

Domínguez, Iliana. *Elaboración del Perfil de Competencias del Especialista WEB*. http://www.gestiopolis.com/recursos5/docs/rrhh/perficompe.htm

Microsoft Corporation, *Guía de administración de riesgos de seguridad*, http://www.microsoft.com/latam/technet/articulos/adminriesgos/srsgch02.mspx.

Stoneburner, Gary. *Risk Management Guide for Information Technology Systems*, NIST Special Publication 800-30.

IT Governance Institute, IT Control Objectives for Sarbanes-Oxley, Segunda Edición Setiembre 2006.

16.2 Sitios Oficiales en Internet

→ Microsoft Corporation.
www.microsoft.com

→ Biblioteca Monografías
www.monografias.com/

→ The Institute of Internal Auditor
www.theiia.org

→ National Institute of Standards and Technology
www.nist.gov

→ ISACA
www.isaca.org

→ Audinet
www.audinet.org

→ Deloitte
www.deloitte.com

→ Price Waterhouse and Coopers
www.pwc.com

→ Diccionario de la Real Academia Española
www.rae.es

→ Diccionario Wikipedia
www.es.wikipedia.org

17 Anexos

Anexo 1 Memorando de Planificación Preliminar

Anexo 2 Carta Inicio Auditoría

Anexo 3 Conocimiento del Negocio

Anexo 4 Conocimiento del área de TI

Anexo 5 Análisis de Riesgos

Anexo 6 Programa de Auditoría

Anexo 7 Formato Recomendaciones