AAT1965

UNIVERSIDAD CATÓLICA ANDRÉS BELLO

VICERRECTORADO ACADÉMICO

DIRECCIÓN GENERAL DE ESTUDIOS DE POSTGRADO

AREA DE INGENIERÍA

Postgrado en Gerencia de Sistemas de Información

Trabajo de Grado de Maestría

Evaluación del Desarrollo de los Fundamentos Teóricos de Seguridad de la Información en la Banca Comercial y Universal de Venezuela

presentado por

Palacios Díaz, Juan Carlos

para optar al título de

Magister en Gerencia de Sistemas de Información

Tutor

Pereira, Wilmer

Caracas, Noviembre del 2008

DEDICATORIA

A Juan, para que sirva de ejemplo en tu vida hijo, eres lo mejor, futuro…

A Faride, sí pude bella, gracias por creer ciegamente en mí y estar a mi lado todos los días de mi vida, amor…

A mis padres, sencillamente nunca tuve mejores consejos ni guías, gracias por hacerme el hombre que soy, espero se sientan tan orgullosos de mí como yo lo estoy de ustedes, sabiduría…

A mis hermanos, sin ustedes sería un ser incompleto, apoyo…

A mis antepasados, gracias por cuidarme siempre, luz…

A mis sobrinos, son mi felicidad hasta en los momentos más difíciles siempre hay una sonrisa, alegría…

Simplemente este esfuerzo se los dedico, constancia…

AGRADECIMIENTOS

A la Profesora Soledad Díaz Heredia por invertir su tiempo y dedicación hasta ayudarme a convertir estas páginas en un Trabajo de Grado de Maestría de la Universidad Católica Andrés Bello.

Al Profesor Emmanuel López, sus consejos están plasmados a lo largo de todo el trabajo, Ud. me ha devuelto la fe en la sabiduría y los docentes.

A mi tutor el Profesor Wilmer Pereira, por apoyar este proyecto y creer.

A IT Servicios de Venezuela, nunca han dejado de apostar en mí.

A todos los profesionales de las instituciones financieras que aportaron su grano de arena y han hecho de este trabajo una realidad.

A mis compañeros Janeth Perez, Carla Iglesias, Daniel Acuña, Eleodina Ramirez, quienes trabajamos juntos por lograr nuestras metas, sin Uds. no estaría aquí.

A Maria Alejandra Pirona, siempre has estado con tu amistad y ahora con tus consejos, gracias por apoyarme.

A Douglas Angulo, por brindar su mano amiga y facilitar el trabajo.

A todos gracias totales.

ÍNDICE

INDICE DE FIGURAS ..... **VI**

INDICE DE TABLAS ..... **IX**

INDICE DE TABLAS ..... **IX**

RESUMEN ..... **- 1 -**

INTRODUCCIÓN ..... **- 2 -**

CAPITULO I ..... **- 4 -**

CONTEXTUALIZACIÓN Y DELIMITACIÓN DEL PROBLEMA ..... - 4 -

INTERROGANTES DE LA INVESTIGACIÓN ..... - 8 -

OBJETIVO GENERAL ..... - 9 -

OBJETIVOS ESPECÍFICOS ..... - 9 -

JUSTIFICACIÓN ..... - 9 -

CAPITULO II ..... **- 12 -**

ANTECEDENTES ..... - 12 -

FUNDAMENTOS TEÓRICOS ..... - 15 -

Ciclo de Seguridad de la Información ..... *- 16 -*

Controles de Acceso ..... *- 17 -*

Telecomunicaciones y seguridad en redes ..... *- 18 -*

Prácticas en Gerencia de Seguridad de la Información ..... *- 19 -*

Seguridad en el Desarrollo de Sistemas y Aplicaciones ..... *- 64 -*

Criptografía ..... *- 76 -*

Modelos y arquitecturas de seguridad ..... *- 76 -*

Seguridad de Operaciones ..... *- 77 -*

Planificación de Continuidad de Negocio (BCP) y Recuperación de Desastres (DRP) ..... *- 77 -*

Incidentes y Leyes ..... *- 103 -*

CAPITULO III ..... **- 123 -**

TIPO Y DISEÑO DE LA INVESTIGACIÓN ..... - 123 -

POBLACIÓN Y MUESTRA ..... - 124 -

DEFINICIÓN DE LAS VARIABLES ..... - 125 -

INSTRUMENTO DE RECOLECCIÓN DE DATOS ..... - 127 -

CONFIABILIDAD Y VALIDEZ DEL CUESTIONARIO ..... - 128 -

TÉCNICAS PARA EL ANÁLISIS DE LOS DATOS ..... - 129 -

PROCEDIMIENTO ..... - 129 -

CAPÍTULO IV ..... **- 130 -**

RESULTADOS ..... - 130 -

CONCLUSIONES ..... - 150 -

RECOMENDACIONES ..... - 152 -

REFERENCIAS BIBLIOGRÁFICAS ..... **- 154 -**

APÉNDICE A ..... **- 160 -**

INSTRUMENTO DE RECOLECCIÓN DE DATOS ..... **ERROR! BOOKMARK NOT DEFINED.**

APÉNDICE B ..... **- 161 -**

VALIDACIÓN DE EXPERTOS ..... - 161 -

INDICE DE FIGURAS

Figura 1. Porcentaje de penetración Internet en la población Venezolana. ..... - 5 -
Figura 2. Principales usos de Internet en Venezuela ..... - 6 -
Figura 3. Triangulo de Seguridad de la Información. ..... - 15 -
Figura 4. Ciclo de Seguridad de la Información. ..... - 17 -
Figura 5. Integración de algunas piezas en un modelo de Seguridad de la Información. ..... - 20 -
Figura 6. Jerarquía de Políticas, estándares y procedimientos. ..... - 24 -
Figura 7. Relación entre los distintos componentes de seguridad ..... - 26 -
Figura 8. Puntos de Acción para Mitigación de Riesgo. ..... - 51 -
Figura 9. Metodología de Mitigación del Riesgo. ..... - 54 -
Figura 10. Controles Técnicos de Seguridad. ..... - 55 -
Figura 11. Implementación de controles y riesgo residual ..... - 57 -
Figura 12. Modelo Cascada. ..... - 66 -
Figura 13. Modelo Cascada Modificado con Validación y Verificación. ..... - 67 -
Figura 14. Modelo Espiral. ..... - 68 -
Figura 15. Componentes Seguridad Ciclo de Vida de Software. ..... - 70 -
Figura 16. Interrupción y Riesgo. ..... - 93 -
Figura 17. Ventana de tiempo para la recuperación. ..... - 94 -
Figura 18. Resultados de la Aplicación del Instrumento ..... - 130 -
Figura 19. Distribución por nivel de Desarrollo en la Gestión del Riesgo Informático. - 131 -
Figura 20. Distribución por nivel de Desarrollo de Políticas, Estándares y Procedimientos. ..... - 132 -
Figura 21. Distribución por nivel de Desarrollo de la Organización de la Seguridad Informática. ..... - 132 -
Figura 22. Distribución por nivel de Desarrollo de la Seguridad Física y Ambiental... - 133 -
Figura 23. Distribución por nivel de Desarrollo de la Clasificación de la Información. - 133 -

Figura 24. Distribución por nivel de Desarrollo de la Seguridad en Recursos Humanos. ..... - 134 -
Figura 25. Distribución por nivel de Desarrollo en Control de Cambios. ..... - 134 -
Figura 26. Distribución por nivel de Desarrollo en Segregación de Funciones. .. - 135 -
Figura 27. Distribución por nivel de Desarrollo en la Separación de Desarrollo y Producción. ..... - 135 -
Figura 28. Distribución por nivel de Desarrollo en Gestión de Servicios de Terceros. - 136 -
Figura 29. Distribución por nivel de Desarrollo en Planificación y Aceptación de Sistemas. ..... - 136 -
Figura 30. Distribución por nivel de Desarrollo en Protección Contra Código Malicioso. ..... - 137 -
Figura 31. Distribución por nivel de Desarrollo en Respaldos. ..... - 137 -
Figura 32. Distribución por nivel de Desarrollo en Gestión de la Seguridad en Redes. - 138 -
Figura 33. Distribución por nivel de Desarrollo en la Manipulación de Medios. - 138 -
Figura 34. Distribución por nivel de Desarrollo en Intercambio de Información. - 139 -
Figura 35. Distribución por nivel de Desarrollo en Servicios de Comercio Electrónico. ..... - 139 -
Figura 36. Distribución por nivel de Desarrollo en Monitoreo y Control. ..... - 140 -
Figura 37. Distribución por nivel de Desarrollo en Gestión de Acceso de Usuarios. ... - 140 -
Figura 38. Distribución por nivel de Desarrollo en Control de Acceso a Sistemas Operativos. ..... - 141 -
Figura 39. Distribución por nivel de Desarrollo en Control de Acceso a Redes. . - 141 -
Figura 40. Distribución por nivel de Desarrollo en Control de Acceso a Aplicaciones. - 142 -
Figura 41. Distribución por nivel de Desarrollo en Computación Móvil y Tele-Trabajo. ..... - 142 -
Figura 42. Distribución por nivel de Desarrollo en Requerimientos de Seguridad. - 143 -

Figura 43. Distribución por nivel Desarrollo Procesamiento Correcto de Aplicaciones. ..... - 143 -
Figura 44. Distribución por nivel de Desarrollo en Controles Criptográficos. .... - 144 -
Figura 45. Distribución por nivel Desarrollo en Seguridad de Sistemas de Archivos. . - 144 -
Figura 46. Distribución por nivel de Desarrollo en Seguridad de Procesos de Desarrollo y Soporte. ..... - 145 -
Figura 47. Distribución por nivel de Desarrollo en Manejo de Incidentes. ..... - 145 -
Figura 48. Distribución por nivel de Desarrollo en Gestión de Continuidad del Negocio. ..... - 146 -
Figura 49. Distribución por nivel de Desarrollo de Compromisos Legales – SUDEBAN. ..... - 147 -
Figura 50. Distribución por nivel de Desarrollo en Cumplimiento de Políticas, Estándares y Procedimientos. ..... - 147 -
Figura 51. Distribución por nivel de Desarrollo en Auditoria Interna y Externa. - 148 -
Figura 52. Pertenencia de la Banca Comercial y Universal a organizaciones internacionales. ..... - 148 -
Figura 53. Cumplimiento de Normas Internacionales Tipo ISO. ..... - 149 -

INDICE DE TABLAS

Tabla 1. Áreas a cubrir por las políticas de seguridad ..... - 23 -
Tabla 2. Amenazas Humanas. ..... - 30 -
Tabla 3. Criterios de Seguridad. ..... - 33 -
Tabla 4. Definición de la probabilidad. ..... - 35 -
Tabla 5. Valores de Impacto. ..... - 36 -
Tabla 6. Valor de la clase de Impacto ..... - 36 -
Tabla 7. Ventajas y desventajas del Riesgo Cuantitativo y Cualitativo ..... - 38 -
Tabla 8. Impacto y probabilidad. ..... - 39 -
Tabla 9. Listado de Niveles de Riesgo. ..... - 40 -
Tabla 10. Valor de exposición de la confidencialidad e Integridad. ..... - 41 -
Tabla 11. Valor de exposición de la disponibilidad. ..... - 42 -
Tabla 12. Como se determinan los valores de impacto. ..... - 42 -
Tabla 13. Ejemplo de Valores de Clases de Impacto Detallado. ..... - 43 -
Tabla 14. Evaluación de vulnerabilidades. ..... - 44 -
Tabla 15. Evaluación del valor de la probabilidad. ..... - 44 -
Tabla 16. Evaluación de la efectividad de los controles. ..... - 45 -
Tabla 17. Ejemplo de la Lista Detallada de Riesgo. ..... - 46 -
Tabla 18. Ranking de Resumen Cualitativo. ..... - 46 -
Tabla 19. Cálculo del SLE. ..... - 49 -
Tabla 20. Ejemplos de SLE. ..... - 49 -
Tabla 21. Cuantificación del ARO. ..... - 49 -
Tabla 22. Ejemplo de ALE. ..... - 50 -
Tabla 23. Seguridad de TI en SDLC. ..... - 71 -
Tabla 24. Tipos de control de aplicaciones ..... - 73 -
Tabla 25. Ejemplo de Estructura Comité de Dirección. ..... - 82 -
Tabla 26. Ejemplo de Riesgo. ..... - 92 -
Tabla 27. Principios de Basilea II y los aspectos de IT. ..... - 116 -
Tabla 28. Variables de la Investigación ..... - 125 -
Tabla 29. Relación de las variables con mejores prácticas ..... - 127 -

RESUMEN

El objetivo de esta investigación, es evaluar el desarrollo de la aplicación de los fundamentos teóricos de seguridad de la información en la Banca Comercial y Universal de Venezuela, con base en las mejores prácticas conocidas como la Norma Técnica ISO 17799:2005 y Cuerpo Teórico de la Certificación CISSP de ISC2.

Para el logro de este objetivo se planteó una investigación de tipo documental y de campo, usando un diseño no experimental transeccional, ya que se realizó en un momento preciso del tiempo y no se manipularon las variables. La población estuvo definida por las organizaciones pertenecientes a la Banca Comercial y Universal de Venezuela y la muestra fue no probabilística con selección subjetiva de individuos a juicio del investigador cuyas características cumplían con: personal profesional especializado, perteneciente de la gerencia de seguridad de la información de su organización.

Las variables de estudio se midieron a través de un instrumento, dicho instrumento fue un cuestionario aplicado en forma directa sobre los individuos pertenecientes a la muestra, el instrumento estuvo constituido por las 13 variables de la investigación, alguna de ellas con subíndices, en total se evaluaron 33 ítems con escala de Likert y dos de ellas dicotómicas.

Finalmente se llevo a cabo el análisis de datos, utilizando estadística descriptiva. Del estudio se derivaron las siguientes conclusiones: en cuanto a la evaluación del desarrollo de la aplicación de los fundamentos teóricos en seguridad de la información en la Banca Comercial y Universal de Venezuela según la percepción de los encuestados, la mayoría de las instituciones se encuentran entre bastante y completamente desarrollados. En cuanto al estado de las variables técnicas en relación a las variables de gestión, las primeras se encuentran más desarrolladas, motivo por el cual es necesario apoyar la gestión de seguridad de la información.

INTRODUCCIÓN

La información, entendiéndola como un conjunto de datos cuya función es proporcionar conocimiento, es uno de los activos más importantes no solo para empresas y organizaciones, si no para cada individuo y su protección juega un papel importante independientemente del fin. Los sistemas informáticos hacen uso de esa información para realizar tareas en cualquier sector de la sociedad. No es una noticia nueva el alcance y el crecimiento de los medios informáticos en el mundo y Venezuela no es la excepción, según Tendencias Digitales (2008), para el año 2007 la penetración de Internet era de 19,70% y el número de usuarios calculado en 5.400.000. Los sistemas computacionales han pasado de ser una herramienta a una necesidad, donde en cualquier ámbito de la sociedad, su uso se ha masificado para ayudar a las personas a agilizar tareas, dando nuevas oportunidades para hacer mejor uso del tiempo.

Pero así como no es nuevo el uso de sistemas de computación para llevar a cabo necesidades básicas de negocios, organizaciones y corporaciones, la utilización de estos sistemas para efectuar actividades delictivas tampoco lo es. El empleo indebido de los sistemas informáticos, redes e Internet ha creado hechos delictuosos, generando en los diferentes actores de la sociedad pérdidas de importantes sumas de dinero, reputación, confianza e incluso llevar a gobiernos a crisis diplomáticas como fue el caso de las relaciones entre Venezuela y Colombia, por causa de las computadoras incautadas a un miembro de las Fuerzas Armadas Revolucionarias de Colombia (Interpol,2008).

Los hechos del 11 de Septiembre del 2001 marcaron un hito en el modo de ver la seguridad, esto no quiere decir que antes no se hayan realizado avances significativos en el área, pero si se han tomado medidas con mas empeño y control a partir de estos sucesos. La preocupación creciente en Seguridad de la Información tiene múltiples vectores, y realizar trabajos en el área requiere especialización y entrenamiento tanto del lado agresor como de la victima.

En Venezuela, el sector Bancario siempre ha estado a la vanguardia en el tema de la Seguridad de la Información, sin embargo es de opinión del autor de este trabajo basado en su experiencia que, no se había enfocado la seguridad como un todo y se

realizaban soluciones específicas como cortafuegos, listas de acceso, etc. Es en los últimos años con el conocimiento, regulaciones y lineamientos tanto estatales como organizacionales que la Seguridad de la Información se ha englobado con más control y fortaleza.

El motivo principal del presente trabajo es evaluar la aplicación del desarrollo de los fundamentos teóricos de seguridad de la información, para ello se escogieron individuos que cumplieran con criterios definidos por el investigador pertenecientes al total de instituciones, según la Asociación Bancaria de Venezuela (2007), para el momento de realización de la investigación la población era de treinta y siete (37) organizaciones pertenecientes a la Banca Comercial y Universal y la muestra fue de catorce (14). Una de las condiciones principales establecidas para poder realizar esta investigación fue no revelar información de nombres de las instituciones a las que se les estaba haciendo la aplicación del instrumento y mantener la confidencialidad en la recepción del instrumento. Previa la entrega del instrumento se hizo contacto con el personal de la gerencia correspondiente a Seguridad de la Información en cada una de las organizaciones para hacer un resumen corto, exposición de motivos y posteriormente envío del material de evaluación a través de correo electrónico. De las catorce instituciones entrevistadas vía cuestionario, doce respondieron, una se negó por aspectos relacionados con la sensibilidad de la información y el último simplemente no contesto.

Con base en lo expuesto anteriormente el presente Trabajo de Grado de Maestría, trata en el primer capítulo los objetivos y el planteamiento del problema, seguido del marco teórico, en el segundo capítulo, donde se abarcan los fundamentos conceptuales en Seguridad de la Información, enfocándose en dominios poco tratados en los trabajos actuales. El marco metodológico, se expone en el tercer capítulo explicando las características del diseño y tipo de la investigación, culminando con el cuarto capítulo donde se muestra y analizan los hallazgos para generar las conclusiones y recomendaciones, en consecuencia respondiendo las interrogantes planteadas.

CAPITULO I
EL PROBLEMA

Contextualización y Delimitación del Problema

El mundo de hoy presenta grandes retos. La globalización apoyándose en las infraestructuras de tecnologías y comunicaciones (TIC) hace que la información fluya sin importar las barreras de la distancia, idiomas o tiempo. Una muestra del avance global en materia de negocios y servicios a través de las TIC se puede identificar a través de Internet, donde se realizan actividades bancarias, compras de cualquier objeto e incluso educación a distancia (eLearning) desde un computador en casa o en cualquier lugar desde donde el usuario pueda conectarse a la red. El hecho de romper las barreras de la distancia a través de las comunicaciones brinda la oportunidad de acceder la información cuando se necesite, pero creando una dependencia inseparable TIC-Organización.

Así como la masificación de las TIC ha traído múltiples beneficios, también ha desviado la razón de su uso en algunos casos para actividades de índole malicioso, motivo por el cual se han desarrollado mecanismos para la protección de la información. Este es el foco principal de la Seguridad de la Información.

Debido al anonimato, complejidad y dificultad en el seguimiento y rastreo, los medios y redes informáticas constituyen un vehículo perfecto para las actividades delictivas. Las pruebas, rastros o huellas no son fáciles de recolectar, lo que reduce los riesgos a los infractores y dificulta la tarea de quienes deben combatirlos. Hoy día, este tipo de delitos es un verdadero problema, cuyos efectos sobre la economía, los negocios y la vida privada pueden llegar a ser tan invisibles como devastadores (Tablante,2001). En Venezuela hay varias causas de delitos informáticos, entre los que se pueden resaltar:

- Gran cantidad de usuarios de Internet en el mundo con alrededor de 6.676.120.288 (IWS,2008), y en Venezuela aproximadamente, 5.400.000 ínter nautas. Ver Figura 1 (Palazzolo,2008).

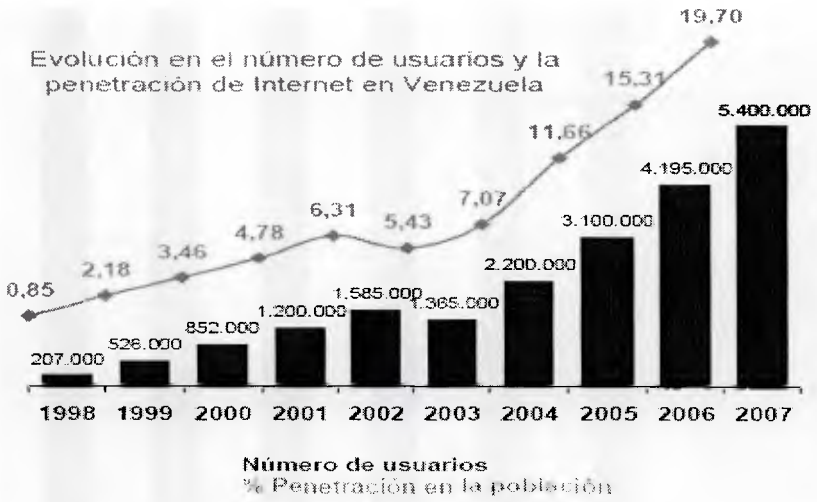

Figura 1. Porcentaje de penetración Internet en la población Venezolana.
Fuente: Tendencias Digitales 2008.

- Uso significativo de comercio electrónico en Venezuela. Para el año 2005 se estimó en unas 286.000 personas, haciendo uso de un gasto promedio de US$115, según estas cifras las compras realizadas por consumidores venezolanos en Internet ascendieron a unos US$ 132.000.000 (TendenciasDigitales,2006).
- Incremento en el uso de Internet para operaciones bancarias, del 3.0% de la población al 12% (Palazzolo,2008), ver Figura 2.
- Dependencia de negocios en las infraestructuras tecnológicas y comunicacionales.
- Tendencia de negocios a nivel nacional e internacional a orientar productos y servicios a través de Internet.
- Actividades delictivas sumamente lucrativas, para las organizaciones que llevan a cabo estas tareas las ganancias son más altas que el tráfico de drogas (El Nacional,2007).
- El dinamismo de las tecnologías y la competencia, resta tiempo para estar a la vanguardia y poder enfocar la importancia en Seguridad de la Información, dando pie para conseguir nuevas vulnerabilidades y formas de ataque.

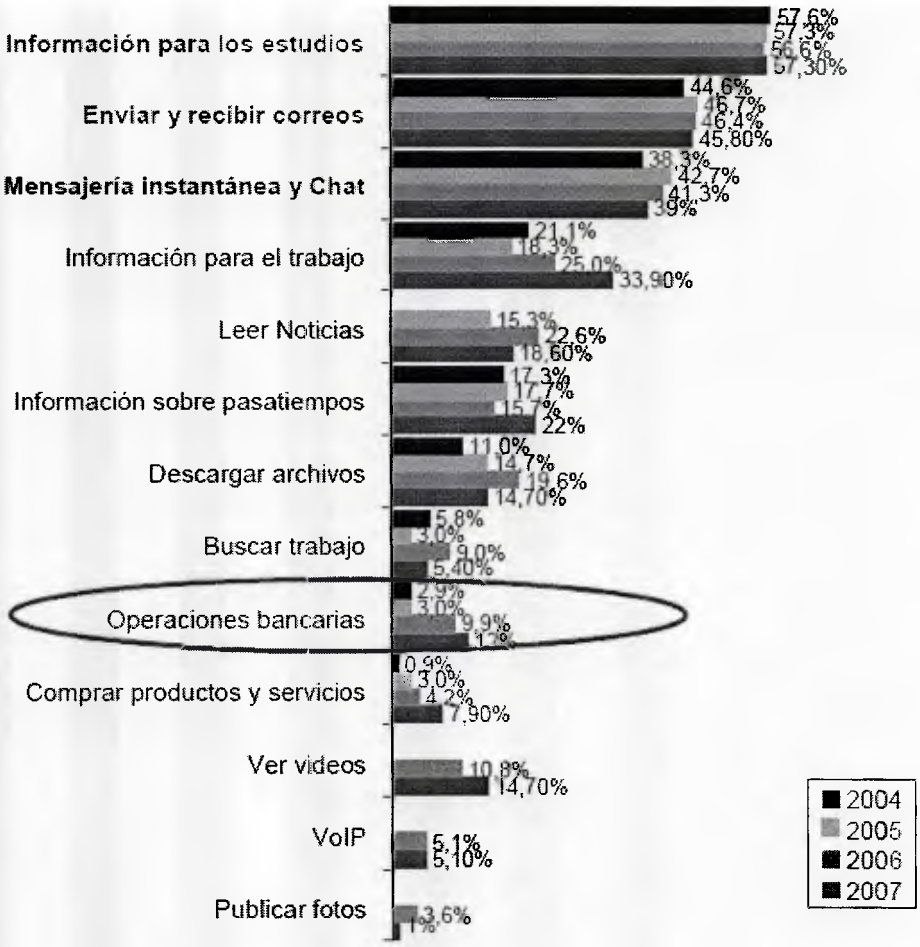

Figura 2. Principales usos de Internet en Venezuela

Fuente: Tendencias Digitales 2008.

- En Venezuela existen las leyes que fomentan el uso de las TIC y protegen a los usuarios en caso de delitos, pero dichas leyes pierden validez por su novedad y la falta de conocimiento en el área leyes-Seguridad de la Información. Algunas de estas leyes serán abordadas en el marco teórico.
- El autor de este trabajo de grado de maestría, tiene 10 años de experiencia en el área, en los cuales ha detectado la complejidad para dar rumbo a la Seguridad de la Información en las organizaciones, ya que se debe contar con personal sumamente especializado, muy solicitado y poco disponible en el mercado.

Las actividades delictivas traen consecuencias incalculables como: pérdida de credibilidad, confianza, reputación, etc., siendo irreversibles en algunos casos para personas y organizaciones. Entre las consecuencias tangibles de las actividades delictivas se puede mencionar, entre otros:

- Aumento en la cantidad de delitos informáticos en Venezuela (Tablante,2001). Para el año 2000 se reportaron 618 y para los primeros 2 meses del año 2001 ya se habían detectado 295, siendo afectadas 22 instituciones financieras. De acuerdo a (RNV,2007) aunque no se tienen números precisos en cuanto a delitos informáticos, se ha visto un crecimiento en quejas y reclamos (área bancaria), y se cree que la cantidad y los montos afectados han ido aumentando considerablemente.
- Piratería y ausencia de protección a los derechos de autor y propiedad intelectual, para el año 2006, en Venezuela alrededor del 85% de comercio audiovisual son copias ilegales o piratas (Unionradio,2006).
- Pérdidas cuantiosas tanto para las organizaciones privadas como para el gobierno, las mermas en software para PC por piratería en Venezuela para el año 2006 fueron alrededor de US$ 307.000.000, formando parte de la lista de los veinte países con la tasa más alta de piratería (BSA,2007).
- Pedofilia o pornografía Infantil, considerada como un delito informático, existen miles de páginas Web y en Venezuela se trafican hasta 8 mil imágenes al mes (RNVAN,2007).
- Conflicto en las relaciones diplomáticas entre países, como fue el caso entre Venezuela y Colombia a causa de las computadoras incautadas a las Fuerzas Armadas Revolucionarias de Colombia en un operativo militar (INTERPOL,2008).

Integrar todos los dominios y darle dirección a la Seguridad de la Información en una organización no es una tarea fácil, por cuanto se requiere conocimiento, experiencia y directrices organizacionales. Las empresas y su personal deben considerar dominios de conocimiento en Seguridad de la Información como: Planes de Continuidad de Negocio y Recuperación de Desastres, Basamentos Legales, Desarrollo de

Aplicaciones Seguras, Controles de Acceso, Criptografía, entre otros, para poder prevenir, detectar y minimizar el impacto de los hechos delictivos.

Los dominios considerados como poco desarrollados en trabajos de investigación se abarcarán con mayor profundidad en este trabajo. El investigador se apoyará en la Norma Técnica ISO 17799 "Tecnologías de Información – Técnicas de Seguridad – Código de Práctica para la Gestión de Seguridad de la Información" y en el "Common Body of Knodledge" para la certificación internacional CISSP de ISC^2 (http://www.isc2.org) como bases fundamentales para los dominios teóricos a cubrir.

En consecuencia, el presente Trabajo de Grado de Maestría tiene como propósito analizar los fundamentos teóricos en la Seguridad de la Información, y evaluar el desarrollo de estos fundamentos en la Banca Comercial y Universal de Venezuela. Se pretende que el Trabajo de Grado de Maestría sirva como guía referencial al personal involucrado en Seguridad de la Información, de manera tal que pueda llevar la conducción de sus actividades gerenciales apoyado en las mejores prácticas existentes.

Interrogantes de la Investigación

- ¿Cuales son los fundamentos teóricos en Seguridad de la Información en la organización?
- ¿Por qué es importante el desarrollo de buenas prácticas gerenciales de seguridad?
- ¿Cómo se puede planificar la seguridad de la información en la organización?
- ¿Cómo se debería aplicar la seguridad de la información en el desarrollo de sistemas y aplicaciones?
- ¿Para que se usa la planificación de continuidad del negocio y recuperación de desastres?
- ¿Cuáles son las leyes y regulaciones que aplican para la seguridad de la información?

Objetivo General

- Evaluar la aplicación del Desarrollo de los Fundamentos Teóricos de Seguridad de la Información en la Banca Universal y Comercial de Venezuela basado en la Norma Técnica ISO 17799:2005.

Objetivos Específicos

- Analizar los Fundamentos Teóricos en Seguridad de la Información.
- Determinar un ciclo de Seguridad de la Información.
- Conocer las mejores prácticas en Gerencia de Seguridad de la Información.
- Estudiar las bases de la seguridad en el desarrollo de sistemas y aplicaciones.
- Conocer los planes de Continuidad de Negocio (BCP) y Recuperación de Desastres (DRP).
- Identificar las leyes venezolanas relacionadas con Seguridad de la Información.
- Situar el estado de los fundamentos teóricos basado en el ISO 17799:2005 en la Banca Comercial y Universal de Venezuela.
- Identificar la relación entre Bancos Internacionales/Nacionales con el estado de los fundamentos teóricos.
- Establecer la relación entre el estado de los fundamentos teóricos de Seguridad de la Información y certificaciones internacionales como ISO.

Justificación

La información es un bien esencial para personas y organizaciones ya sean públicos o privados, puede existir en muchas maneras, estar impresa o escrita en papel, almacenada electrónicamente o transmitida por diferentes medios de comunicación y dependiendo de su sensibilidad, se deben aplicar medidas apropiadas para su protección.

La Seguridad de la Información es la protección de la información de un amplio rango de amenazas con el fin de asegurar la continuidad del negocio, minimizar riesgos y maximizar retornos de inversión y oportunidades de negocio.

La información y los procesos, sistemas y redes que la soportan son bienes importantes. Definir, mantener y mejorar la seguridad de la información puede ser esencial para mantener la competitividad, flujo de caja, rentabilidad, cumplimientos legales y la imagen comercial.

Las organizaciones y sus sistemas de información y comunicaciones enfrentan amenazas de un amplio rango de fuentes, incluyendo fraude asistido por computadoras, espionaje, sabotaje, vandalismo, fuego o inundaciones. Causas de daño como código malicioso, hacking de computadoras y los ataques de denegación de servicios vienen siendo más comunes, más ambiciosos y más sofisticados.

Muchos sistemas de información no han sido diseñados para ser seguros. La seguridad lograda a través de medios técnicos es limitada, debe ser soportada por la gerencia y procedimientos apropiados. Identificar que controles deben ser usados requiere una planificación cuidadosa y atención en los detalles. Para poder alcanzar Gerencia en Seguridad de la Información y cumplir con todos estos requerimientos es necesario conocer teóricamente como debe gestionarse la Seguridad de la Información en la organización, conocer su estado y empezar a aplicar las mejoras correspondientes.

A nivel mundial, la certificación internacional CISSP (Certified Information Systems Security Professional) de ISC^2 (http://www.isc2.org), es reconocida como aval para personas competentes dentro del mundo de la Seguridad de la Información, también está , motivo por el cual, en conjunto con la Norma Técnica ISO 17799:2005 se tomarán como base para los fundamentos teóricos en Seguridad de la Información; también esta base servirá para conocer su desarrollo en la Banca Comercial y Universal de Venezuela.

Una vez planteado el problema y las fuentes del basamento teórico, conocer el estado de los fundamentos en Seguridad de la Información, contribuirá con las instituciones financieras y organizaciones interesadas, en aspectos como:

- Conocer la aplicación del desarrollo de los dominios de conocimiento más desarrollados.
- Fortalecer los dominios más débiles.
- Mantener y monitorear los dominios considerados como desarrollados.

- Establecer la consistencia y relación entre los dominios.
- Definir una base para el nivel de la seguridad organizacional, basada en información propia.
- Enunciar algunos basamentos legales que se deben cumplir.
- Establecer lineamientos confiables basados en mejores prácticas.

Existen aportes significativos para las Universidades y en particular la Universidad Católica Andrés Bello como serían:

- Especificar un ciclo de Seguridad de la Información.
- Necesidad de aportar mayor foco en la Gestión de la Seguridad de la Información.
- Apuntar objetivos de aprendizaje a nivel académico en áreas detectadas como poco desarrolladas, constituyendo un aporte con necesidades inmediatas en las organizaciones (al menos en la Banca Comercial y Universal).
- Conocer la relación existente entre los dominios de la Seguridad de la Información.
- Servir como punto de partida y referencia para profesores y estudiantes en la búsqueda y desarrollo de nuevos trabajos de investigación en el área de Seguridad de la Información, ya que existen fundamentos teóricos extensos y nuevos que sirven para profundizar en su complejidad y desarrollo intelectual.

Debido al contacto laboral que tiene el investigador con personal clave en el área de Seguridad de la Información de la Banca Comercial y Universal de Venezuela, es posible desarrollar el trabajo en esta área. Así se considera que este trabajo de investigación se podría convertir en un modelo e instrumento para el desarrollo de la Seguridad de la Información organizacional.

CAPITULO II
MARCO TEÓRICO

Antecedentes

La Seguridad de la Información se ha estudiado desde hace mucho tiempo. Ya en 1918, se usaban equipos comerciales para enviar y recibir textos cifrados (Perera,2005), o para dar respuesta reactiva a problemas no detectados en el desarrollo de sistemas, aplicaciones, hardware, etc. Hoy día se puede palpar este fenómeno cuando al usar los computadores para el trabajo diario se observan alertas de actualización del sistema por vulnerabilidades detectadas.

Es en los últimos años cuando se ha tratado de ver la seguridad de la información desde un punto de vista general, y donde se trata de hacer un trabajo preventivo para mitigar estos problemas y vulnerabilidades. Para poder entender este nuevo paradigma de trabajo es importante aplicar la teoría de Seguridad de la Información que comprende los siguientes dominios:

- Practicas Gerenciales de seguridad de la información.
- Controles de acceso.
- Modelos y arquitecturas de seguridad de la información.
- Seguridad física.
- Seguridad en redes y telecomunicaciones
- Criptografía.
- Continuidad de negocio.
- Leyes, investigación y ética.
- Seguridad en el desarrollo de aplicaciones y sistemas.
- Seguridad en las operaciones.

Debido al amplio espectro que se pretende abarcar, es posible que existan "huecos" que no han sido cubiertos en el área de Seguridad de la Información en las organizaciones venezolanas. La información encontrada (en los antecedentes) no cubre totalmente los factores clave mencionados anteriormente, motivo por el cual se ampliarán los fundamentos teóricos considerados necesarios. De la información encontrada investigada se tiene:

- "Elementos Básicos Para Modelos de Seguridad En Organizaciones Venezolanas". Jesús Manuel Hamana Falcón. Universidad Metropolitana. 2003. En este se dan algunos conceptos básicos de modelos de seguridad de la información como son Bell-LaPadula, Clark-Wilson y Harrison-Ruzzo-Ullman. Del trabajo también se entiende que las políticas corporativas y la concientización de los usuarios para desarrollo de la seguridad de la información juegan un papel crucial. El trabajo brinda aporte teórico para el factor de "Modelos y arquitecturas de seguridad de la información" y "Practicas Gerenciales de la Seguridad"
- "Implantación de una red privada virtual (VPN) para el acceso seguro y controlado al sistema de información del sector eléctrico venezolano". Pablo José Echenique Salas. Universidad Central de Venezuela. 2004. En este trabajo de postgrado se encuentra la teoría para el desarrollo y la implantación de una Red Privada Virtual, las cuales son creadas para aprovechar las redes que se conectan hacia Internet y cifrar la información entre organizaciones conectadas a esta, abaratando los costos y manteniendo la integridad, confidencialidad y disponibilidad de la información. Este trabajo ayuda en el aporte intelectual a los factores de "Seguridad en redes y telecomunicaciones" y "Criptografía".
- "Evaluación de seguridad de una institución financiera mediante la ejecución de un estudio de penetración interno y externo a su infraestructura tecnológica". Víctor E. Pittol M. Universidad Central de Venezuela. 2004. Las pruebas de penetración son análisis que se le realizan a las redes de las organizaciones tanto internas (desde la red interna de la organización) como externas (usualmente desde Internet) para verificar el estado de vulnerabilidad en que se encuentran sus sistemas, el trabajo presenta la metodología usada para llevar a cabo esta tarea con el fin de elevar la seguridad y disminuir los riesgos. Este trabajo de postgrado ayuda en el campo de "Seguridad en redes y telecomunicaciones", "Criptografía" mencionado en los factores anteriores.
- "Estudio de técnicas biométricas para verificación de identidad en sistemas de control de acceso". Marta Rodríguez Martínez. Universidad Central de

Venezuela. 2004. Las técnicas biométricas son usadas para el proceso de autenticación de personas en seguridad de la información, ya que cada ser humano tiene características que lo identifican unívocamente como su huella digital. Este trabajo abarca el estudio de varias técnicas para la identificación de personas, dando apoyo a los factores de "Controles de Acceso".

- "Diseño e implementación de una WAN segura para el Instituto Nacional de Estadística (INE)". Nando A. Vitti V. Universidad Central de Venezuela. 2003. Las organizaciones que se encuentran distribuidas geográficamente alrededor de zonas distantes suelen estar conectadas a través de redes de voz y datos mejor conocidas como "Wide Area Networks" o "WAN". Tal es el caso del Instituto Nacional de Estadística, el uso de este tipo de redes tiene implicaciones de seguridad que no hay que descuidar, cuestiones que se discuten en este trabajo, aportando teóricamente para los factores de "Seguridad en Redes y Telecomunicaciones"

Como se puede ver en los trabajos consultados anteriormente existen estudios puntuales realizados a algunos de los factores de Seguridad de la Información, estos no serán abordados en los Fundamentos Teóricos, para ello se puede ubicar su existencia en las referencias bibliográficas en caso de requerir profundizar el tópico en cuestión.

Fundamentos Teóricos

Para iniciar la comprensión en el tema de Seguridad de la Información se debe conocer su postulado principal (Barge,2002), el cual esta compuesto de tres conceptos: *confidencialidad, integridad y disponibilidad* (ver Figura 3).

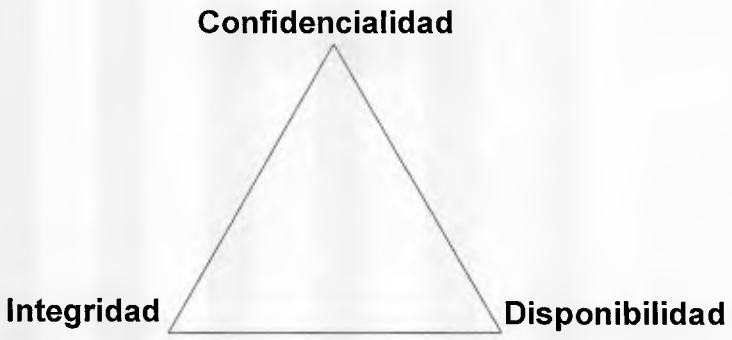

Figura 3. Triangulo de Seguridad de la Información.
Fuente: Elaboración propia.

Todos los controles, amenazas, vulnerabilidades y procesos están sujetos al análisis del postulado principal de Seguridad de la Información, el cual puede verse como un triangulo donde cada vértice esta integrado por sus componentes y lo importante es mantener el equilibrio dependiendo del tipo de seguridad necesitado. Se define cada componente a continuación:

Confidencialidad: previene la revelación del contenido de las comunicaciones, permite garantizar la seguridad aplicada a cada procesamiento de datos y la prevención de revelación no autorizada

Integridad: consiste en asegurar la exactitud y confiabilidad de la información en contra de modificaciones no autorizadas a los datos. Asegurar que los datos recibidos están exactamente según lo enviado por una entidad autorizada (Stallings,2006)

Disponibilidad: asegura el acceso a los datos y recursos informáticos de manera confiable y oportuna por el personal apropiado; garantiza que los servicios estén disponibles cuando sean necesarios.

Otros conceptos relacionados también importantes:

Privacidad: Principio de seguridad que protege la información individual y emplea controles para asegurar que dicha información no sea diseminada o accedida de manera no autorizada (Krutz,2003).Ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión (RAE,2006).

Autenticación: es el proceso de determinar si alguien o algo es, de hecho, quien presenta ser (Entrust,2006). Acción y efecto de autenticar, o sea, autorizar o legalizar algo (RAE,2006).

"Accountability": capacidad de los sistemas para determinar las acciones y comportamiento de individuos dentro del sistema y para identificarlo. Los registros de auditoria y del sistema soportan "accountability" (Krutz,2003)

No Repudiación: brinda protección contra la negación por alguna de las partes relacionadas en una comunicación de haber participado en toda o parte de la comunicación (Stallings,2006)

Ciclo de Seguridad de la Información

Si bien entender el postulado principal de Seguridad de la Información es importante, también lo es comprender el Ciclo de Seguridad de la Información. Se entiende por este al proceso que debe efectuar la organización para cumplir con sus requerimientos de seguridad en las TIC, proteger sus activos de información y mitigar los riesgos informáticos. En la Figura 4, se puede observar como se relacionan varios elementos dentro del Ciclo de Seguridad de la Información. La alineación de las estrategias de IT con las del negocio son los cimientos de la parte tecnológica, de allí se derivan las estrategias y requerimientos de seguridad de la información. La idea es planificar la seguridad creando políticas, estándares y procedimientos por los cuales se van a regir y gobernar los usuarios de las TIC en la organización.

Seguidamente se realiza la valoración del riesgo informático, donde se determina su prioridad y el riesgo tolerable por la organización. Una vez realizada esta valoración se deben realizar las acciones necesarias para aceptar, transferir, ignorar o mitigar el riesgo hasta el nivel acordado.

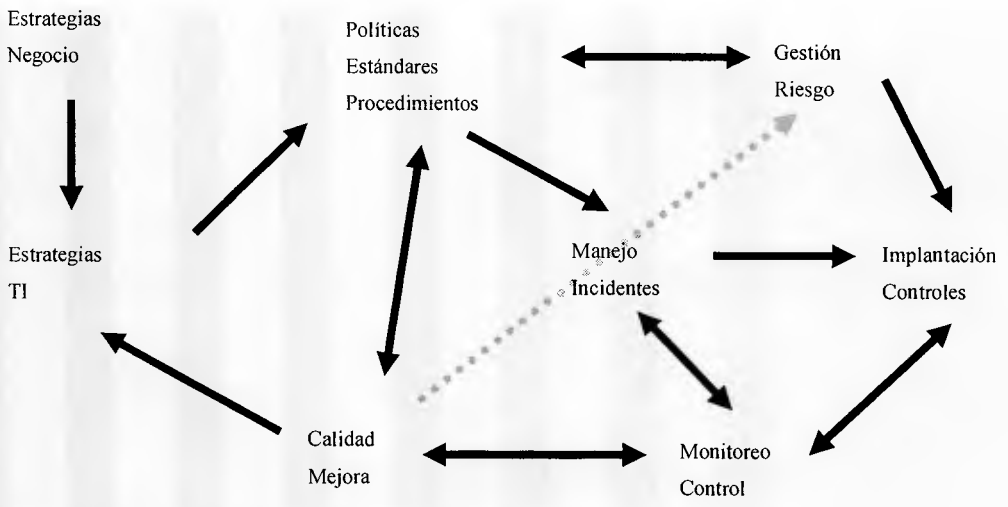

Figura 4. Ciclo de Seguridad de la Información.
Fuente: Elaboración Propia.

A partir de la mitigación se procede con el monitoreo y control de todos los procesos dependientes de Seguridad de la Información y se obtienen valores para los indicadores, es allí cuando toma participación los procesos de mejora continua, auditorias internas y externas y la parte legal, para reanudar el ciclo con la periodicidad explicita en las políticas, estándares y procedimientos.

También es importante el manejo de los incidentes, ya que sirve de ayuda para eventos inesperados, vulnerabilidades nuevas o no identificadas que sea necesaria su mitigación en un periodo de tiempo aceptable.

Este ciclo comprende todos los fundamentos teóricos de Seguridad de la Información, pero una vez entendido el ciclo y clarificados los conceptos que siguen a continuación el lector puede darse una idea de lo que debe abarcar para dar un nivel aceptable a la seguridad de sus medios informáticos.

Una vez entendido el Ciclo de Seguridad de la Información, a continuación se presentan los fundamentos teóricos a cubrir.

Controles de Acceso

Los controles de acceso son una colección de mecanismos que permiten a los administradores de los sistemas ejercer una influencia directa y restrictiva sobre el comportamiento, uso y contenido de un sistema. Permite a la gerencia controlar que

pueden hacer los usuarios, a que recursos pueden acceder y que operaciones pueden realizar en los sistemas (Tipton,2002).

Los controles de acceso aplican un papel importante para la preservación de la confidencialidad, integridad y disponibilidad en los sistemas de información.

Un sujeto es una entidad activa que necesita acceder un objeto, siendo este, una entidad pasiva que posee información o la puede generar. Para que un sujeto pueda acceder un objeto es importante la preservación del principio de seguridad de la información, esto lo hace mediante un proceso de identificación, autenticación, autorización y "accountability", esto se llama controlar el acceso. Este tema tiene amplia información disponible en otros trabajos de investigación motivo por el cual no se estudiará en este trabajo.

Telecomunicaciones y seguridad en redes

La comunicación es un requerimiento del mercado global, por lo tanto es importante entender las redes de comunicaciones y su seguridad, como se relacionan con comunicaciones de voz y datos en términos de distancia:

- Redes locales
- Redes de áreas distantes
- Redes de acceso remoto

Dispositivos que los interconectan como:

- Routers
- Firewalls
- Switches
- Concentradores
- Antenas

Las relaciones con los protocolos como TCP/IP, administración y técnicas de seguridad en las comunicaciones en términos de medidas:

- Preventivas
- Detectivas
- Correctivas

Abarca las estructuras, métodos de transmisión, formatos de transporte y medidas de seguridad usadas para proteger el principio fundamental de seguridad de la información en transmisiones de redes y medios de comunicación públicos y privados. Este tema tiene amplia información disponible en otros trabajos de investigación motivo por el cual no se abarcará en este trabajo.

Prácticas en Gerencia de Seguridad de la Información

Este tema se presenta como uno de los más importantes para el personal gerencial de Seguridad de la información, se explican los conceptos principales para crear las mejores prácticas en la materia.

Existen diversos tipos de controles para administrar la seguridad de la información, estos pueden ser administrativos, técnicos o lógicos y por ultimo los físicos. Dependiendo del tamaño y fin de la organización estos pueden variar considerablemente, los administrativos se refieren al desarrollo de políticas, estándares y procedimientos, seguimientos del personal, concientización de usuarios, procedimientos de controles de cambio, análisis de riesgo, etc. Los controles técnicos o lógicos consisten en los mecanismos de control de acceso, manejo de recursos y passwords, métodos de identificación y autenticación, dispositivos de seguridad y configuración de la infraestructura. Los controles físicos por su parte limitan el acceso de los individuos a la información y las instalaciones, bloqueándolos y retirando de los bienes informáticos material de acceso que no sea necesario (CDROMS, Floppys, etc), protegiendo el perímetro de las instalaciones y monitoreando cualquier intento penetración de intrusos. En este trabajo se hizo énfasis en los controles administrativos.

Marco de Seguridad de la Información

Las organizaciones usan modelos para Seguridad de la Información (SI), estos están compuestos por muchas entidades, mecanismos de protección, componentes lógicos y físicos, procedimientos y configuraciones que trabajan para un fin común. Son como un rompecabezas en el que sus estructuras funcionan como una pieza que encaja en

un contexto general y sin al menos una de ellas, estaría incompleto, la Figura 6 muestra un ejemplo del modelo descrito (Harris,2003).

Una seguridad efectiva requiere focalización y aplicación de todos los componentes y procedimientos, como se mencionó anteriormente algunos son administrativos, otros técnicos y otros físicos pero cada uno tiene un lugar relevante en SI, y para poder llevar a cabo este modelo, se definen capas y metas, estas metas son operacionales, tácticas y estratégicas. Las operacionales son tareas diarias para ayudar a cumplir las metas tácticas, las cuales son objetivos a mediano plazo que ayudan a cumplir las metas estratégicas, llevando la SI al futuro deseado en la organización.

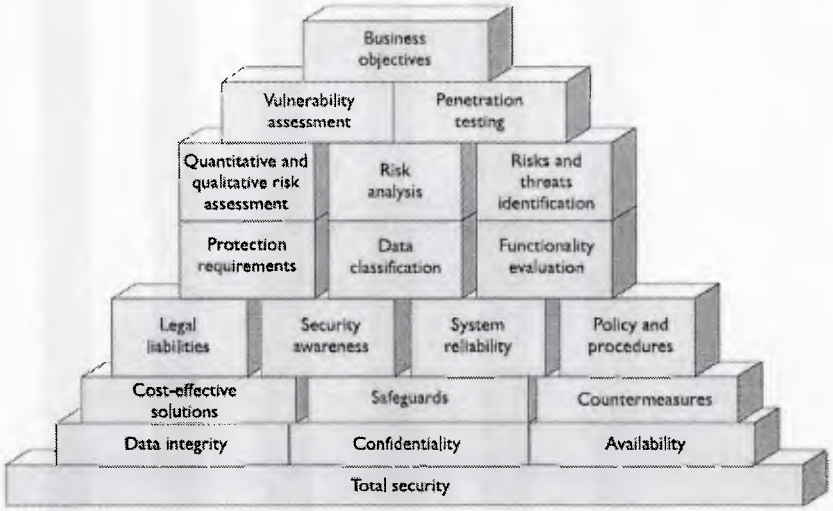

Figura 5. Integración de algunas piezas en un modelo de Seguridad de la Información. Fuente: (Harris,2003)

Políticas, Estándares y Procedimientos

Todas las organizaciones se rigen por directrices o reglas para normar el uso de sus instalaciones, comunicaciones, etc. lo mismo sucede con las Tecnologías de Información, para ello y para soportar las metas estratégicas, la gerencia de Seguridad de la Información crea políticas, estándares y procedimientos. En este proceso de creación es necesario formar un equipo tanto del área de negocio de la organización como de tecnología, para generar políticas claras, que faciliten un equilibrio tanto para seguridad como el uso de la tecnología, el mismo debe ser un equipo

multidisciplinario, la alta gerencia debe revisar las políticas dándoles el suficiente apoyo para que se implementen y actualicen en forma periódica.

Políticas

De acuerdo a Guel (2001) las políticas definen el comportamiento y uso adecuado de los bienes informáticos de la organización. Estas deben establecerse en conjunto con el departamento legal e incluir las sanciones por incumplimiento.

Harris (2003) señala que son una declaración general producida por la gerencia "Senior" (o un comité designado para tal labor) para fijar el rol de la seguridad de la información dentro de la organización.

Es el gobierno por el que se debe regir IT moldeando el uso aceptable de los recursos informáticos en la organización.

Pueden existir diversos tipos de políticas de seguridad dependiendo del tipo de uso que se le da a los recursos, pero la más general debe ser soportada y publicada con el apoyo de la alta gerencia para hacerla cumplir. De nada vale definir políticas de seguridad si no reciben el apoyo adecuado, no llegaran a subsistir en el tiempo. Con las políticas además se trata de dar forma a las metas estratégicas planteadas para Seguridad de la Información, que es función de la gerencia. Las políticas son escritas de manera amplia para abarcar la mayoría de los tópicos en forma general, luego para particularizar y dar énfasis en algún tema específico se definen los estándares, procedimientos, lineamientos base ("Baselines") y guías generales ("guidelines"). Las políticas deben mostrar un balance entre control y productividad, ser concisas y cortas para lograr mejor aceptación y manejabilidad entre el personal.

Proceso de diseño de políticas

1. Escoger un equipo de desarrollo, personas afectadas, personas de soporte, personal de la gerencia, etc.
2. Designar personal que se encargue de la interpretación oficial de las políticas
3. Decidir el alcance (¿Qué está cubierto por las políticas?) y metas de las políticas.
4. Decidir que tan específicas deben ser las políticas

5. Incorporar concientización de usuarios como parte de la orientación de los empleados periódicamente

Tipos de políticas

Reguladoras: son políticas que la organización debe implementar por cumplimiento, regulaciones u otros requerimientos legales. Estas compañías pueden ser financieras, de utilidades públicas u otro tipo de organizaciones de interés público (Krutz,2003).

Consultivas: no son asignadas por mandato pero son fuertemente sugeridas, tal vez con serias consecuencias definidas en caso de no seguirlas. Las compañías con estas políticas buscan que los empleados la consideren por mandato (Krutz,2003).

Informativas: existen simplemente para informar al lector. No existen implicaciones o requerimientos específicos, y la audiencia para esta información puede ser interna o externa.

Las áreas que las políticas de seguridad de la información abarca se pueden visualizar en la Tabla 1.

Estándares

De acuerdo a Harris (2003) los estándares especifican como los productos de hardware y software deben ser usados. A través de los estándares se asegura que tecnologías específicas, aplicaciones, parámetros y procedimientos se usan de manera uniforme en toda la organización.

Los estándares indican el uso de determinada tecnología de manera uniforme. Esta estandarización de procedimientos operacionales puede beneficiar la organización especificando metodologías uniformes a ser usadas por los controles de seguridad. Generalmente son obligatorias y son implementadas en la organización por uniformidad (Krutz,2003).

Baseline

Proveen el mínimo nivel de seguridad necesario por la organización (Harris,2003). En caso que no se encuentre algún procedimiento acerca de la instalación o configuración de alguna aplicación se puede llevar a cabo la misma haciendo

consideración en ciertos aspectos por ejemplo: reforzamiento de los sistemas operativos, deshabilitar servicios no necesarios, etc.

Tabla 1. Áreas a cubrir por las políticas de seguridad

Área	Ejemplo
Controles Accountability	Evidencias de auditorias, revisión de registros de auditoria, automatización de auditoria y configuraciones necesarias
Controles físicos y ambientales	Sistemas de detección de intrusos, mantenimiento sistemas enfriamiento
Controles administrativos	Separación de funciones, chequeo de antecedentes, supervisión, rotación de funciones
Controles de Acceso	Mecanismos de identificación y autenticación, instalaciones biométricas
Criptografía	Cuando usarla, tecnología a usar
Controles Cont. de negocio	Equipo de continuidad, que debe ser documentado
Operaciones Computacionales	Como deben ser instalados y configurados los SO, como deben ser instaladas las aplicaciones, como asegurar las estaciones de trabajo, como reemplazar los HDD
Manejo de Incidentes	Que define un incidente de seguridad, a donde debe ir el reporte, que debe estar en el reporte

Fuente: (Harris,2003)

Lineamientos Generales ("Guideline")

Son similares a los estándares, ellos refieren metodologías para asegurar los sistemas, pero son acciones recomendadas no son obligatorias (Krutz,2003). Los "guidelines" son más flexibles que los estándares y toman en consideración la naturaleza variante de los sistemas de información.

Procedimientos

Los procedimientos son guías detalladas para realizar una actividad en particular, van desde la instalación de computadores personales hasta la configuración detallada de una aplicación en un servidor.

En la Figura 6 se puede visualizar de manera jerárquica la organización de las políticas, estándares y procedimientos, este no debe ser un esquema rígido, lo importante es ubicar al lector en como es su desarrollo.

Una ayuda para facilitar la manipulación y entendimiento de las políticas, estándares, procedimientos, baselines y guidelines es realizar documentos cortos (1 o 2 páginas) que enlacen desde lo más general a lo más detallado, es decir, empezar con

declaraciones generales como las políticas de seguridad de la información hasta llegar a procedimientos detallados.

Figure 1.3 Policy hierarchy.

Figura 6. Jerarquía de Políticas, estándares y procedimientos.
Fuente: (Krutz,2003)

Gerencia del Riesgo

El riesgo es el impacto negativo del ejercicio de una vulnerabilidad, considerando su probabilidad e impacto de ocurrencia. Es el proceso de identificar, determinar, y tomar medidas para reducir el riesgo a un nivel aceptable. En este trabajo se proporciona la base para el desarrollo de un programa eficaz de gestión del riesgo, dando las definiciones y la dirección práctica necesaria para determinar y atenuar los riesgos identificados dentro de los sistemas de TIC.

El objetivo de realizar gerencia del riesgo es permitir a la organización lograr su misión asegurando los sistemas que almacenan, procesan, o transmiten la información de la organización (Stoneburner,2002).

Antes de entrar de lleno en la materia se muestra a continuación algunos conceptos, tomados del Glosario de Seguridad en Internet - RFC 2828 (Shirey,2000), que se utilizarán en el resto del tema:

Vulnerabilidad: defecto o una debilidad en el diseño, puesta en práctica, u operación y gerencia de un sistema que se podrían explotar para violar la política de la seguridad del sistema.

Amenaza: es el potencial para la violación de la seguridad que existe cuando hay una circunstancia, capacidad, acción, o evento que podría ocasionar una brecha de seguridad y causar daño.

Riesgo: es la expectativa de pérdida expresada como la probabilidad que una amenaza particular explotará una vulnerabilidad particular con un resultado dañino particular.

Exposición: es la violación de la seguridad que resulta de la acción de una amenaza. Incluye acceso, daño, interrupción y usurpación.

Contramedidas (salvaguarda): acciones, dispositivos, procedimientos, o técnicas que reduzcan las amenazas, vulnerabilidades o ataques, eliminándolos o previniendo, reduciendo al mínimo el daño puedan causar, o descubriéndolo y divulgándolo para poder tomar acciones correctivas.

Activo: recursos, proceso, producto, infraestructura computacional que la organización ha determinado debe ser protegida.

Un ejemplo de los conceptos anteriores se puede ver en acción cuando una organización sabe que existe algún virus informático (amenaza) que se aprovecha de algún sistema operativo o aplicación (vulnerabilidad), causando daño que a veces puede ser irreparable. La organización al estar consciente del problema (riesgo) y las posibles consecuencias a afrontar (exposición) trata de evitar este virus con algún sistema que minimice el impacto en el negocio (contramedida). En la Figura 7 se pueden ver las relaciones entre los distintos componentes de los que se ha escrito anteriormente.

Una vez comprendidos los conceptos involucrados en la gerencia del riesgo informático, se tomará como base la Guía de Gerencia del Riesgo del NIST (National Institute of Standards and Technology (Stoneburner,2002). Las etapas planteadas a continuación no son rígidas y se toman los aspectos considerados más sencillos para el entendimiento del lector, no son completamente detalladas si desea más información al respecto puede ir directamente a la bibliografía. Las etapas en cuestión son:

1. Valoración del Riesgo.
2. Proceso de mitigación del riesgo.
3. Programa de evaluación de la efectividad.

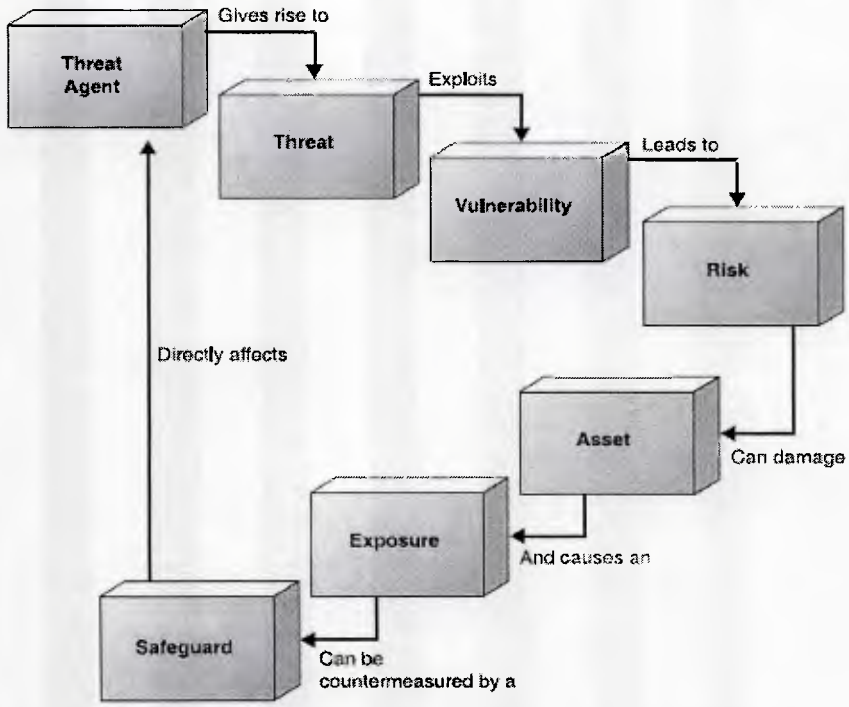

Figura 7. Relación entre los distintos componentes de seguridad
Fuente: (Krutz,2003).

1. Valoración del Riesgo

Es el primer proceso en la Gerencia del Riesgo, las organizaciones usan la valoración para determinar el grado de amenazas potenciales y el riesgo asociado con los sistemas de información. La salida de este proceso ayuda a identificar los controles apropiados para reducir o eliminar el riesgo durante el proceso de mitigación.

Definido el riesgo, como una función de la probabilidad de que una amenaza se ejerza sobre una vulnerabilidad particular y el impacto del resultado de ese evento adverso en la organización. Para determinar esta probabilidad de eventos adversos futuros, las amenazas a los sistemas de TI deben ser analizadas en conjunto con las vulnerabilidades potenciales y sus controles. La metodología planteada por NIST para la valoración del riesgo comprende 7 pasos, a saber:

- Caracterización de los sistemas.

- Identificación de amenazas.
- Identificación de vulnerabilidades.
- Análisis de control.
- Determinar probabilidad.
- Análisis del impacto.
- Determinación del riesgo.

1.1 Caracterización de los sistemas

En la valoración del riesgo para un sistema de TIC, el primer paso es definir el alcance del esfuerzo. En este paso las fronteras de los sistemas son identificados, junto con sus recursos y la información que constituyen los sistemas. Caracterizar un sistema de TIC establece el alcance del esfuerzo de la valoración del riesgo, delinea las fronteras en cuanto a la autorización o acreditación organizacional, y provee información esencial para definir el riesgo.

A continuación se describe la información relativa a los sistemas usada para caracterizar un sistema de TIC y su ambiente operacional, luego se sugieren algunas técnicas que pueden ser usadas para solicitar información relevante a los ambientes de procesamiento de sistemas de TIC.

1.1.1 Información relacionada a los sistemas

Identificar el riesgo de un sistema de TIC requiere un profundo entendimiento del ambiente de procesamiento. La persona o personas quienes forman el equipo de valoración del riesgo deben inicialmente recolectar la información que es clasificada usualmente como:

- Hardware.
- Software.
- Interfaces del sistema (por ejemplo: conectividad interna y externa).
- Datos e información.
- Personas que apoyan en el soporte y usan los sistemas.
- Finalidad del sistema.
- Criticidad del sistema y los datos.

- Sensibilidad del sistema y los datos (relativo al nivel requerido para mantener la CIA).

Adicionalmente la información relacionada al ambiente operacional del sistema de TIC incluyendo sus datos, pero no limitado a lo siguiente:

- Requerimientos funcionales del sistema de TIC.
- Usuarios del sistema.
- Políticas de seguridad de los sistemas que gobiernan los sistemas de TIC.
- Arquitecturas de seguridad de los sistemas.
- Topología de las redes.
- Información acerca de la protección del almacenamiento que salvaguarda la CIA de los sistemas y datos.
- Flujo de la información perteneciente de los sistemas de TIC.
- Controles técnicos usados por los sistemas de TIC.
- Controles administrativos usados por los sistemas de TIC.
- Controles operacionales usados por los sistemas de TIC.
- Seguridad física implementada en el ambiente de procesamiento de los sistemas de TIC.
- Seguridad ambiental implementada en el ambiente de procesamiento de sistemas de TIC.

1.1.2 Técnicas para obtención de información

Cualquiera de las siguientes técnicas puede ser usada para reunir información relevante a los sistemas de TIC con sus fronteras operacionales:

Cuestionarios: el personal puede desarrollar cuestionarios concernientes a la administración y los controles operacionales planeados o usados por el sistema, deben ser distribuidos al personal técnico y no técnico que diseñe y use los sistemas.

Entrevistas: pueden permitir al personal de valoración del riesgo recolectar información útil acerca de los sistemas, las visitas también permiten observar y reunir información acerca de la seguridad física, ambiental y operacional de los sistemas.

Revisión de documentos: documentos de políticas, de los sistemas o cualquier otra documentación relacionada con la seguridad pueden brindar información acerca de los controles de seguridad usados y planeados para los sistemas.

Herramientas de exploración (scanners): métodos técnicos preactivos pueden ser usados para recolectar información de los sistemas eficientemente.

El buen entendimiento del ambiente de los sistemas y el delineamiento de las fronteras de los sistemas son la salida de la caracterización de los sistemas.

1.2 Identificación de amenazas

Las amenazas no presentan riesgo cuando no existen vulnerabilidades que puedan ser aprovechadas. Para determinar la probabilidad de una amenaza, se debe considerar las fuentes de amenazas, vulnerabilidades potenciales y los controles existentes

1.2.1 Identificación de fuentes de amenaza

La meta de este paso es identificar las fuentes potenciales de amenazas y compilarlas en un listado de fuentes potenciales de amenazas (Documento de declaración de amenazas) que son aplicables a los sistemas de TIC que están en evaluación. Las fuentes de amenazas están definidas como cualquier circunstancia o evento con el potencial de causar daño a un sistema de TIC, las fuentes más comunes pueden ser naturales, humanas o ambientales.

1.2.2 Acción y motivación de las amenazas

La motivación y los recursos para realizar un ataque hacen a los humanos fuentes dañinas potenciales. La Tabla 2 presenta la descripción de algunas amenazas comunes por los humanos, sus posibles motivaciones, y los métodos o acciones de amenazas por el cual pueden llevar a cabo un ataque.

Tabla 2. Amenazas Humanas.

Fuente de amenaza	Motivación	Acción de la amenaza
Hacker, cracker	Desafío Ego Rebelión	Hacking Ingeniería social Ingreso de intrusos en sistemas Acceso no autorizado a los sistemas
Criminal de computadoras	Destrucción de información Publicación ilegal de información Beneficio monetario Alteración no autorizada de datos	Crimen computacional Actos Fraudulentos Soborno Spoofing Ingreso de intrusos en sistemas
Terrorista	Chantaje Destrucción Explotación Venganza	Bombas/terrorismo Guerra informática Ataque a sistemas Penetración en sistemas Forzamiento de sistemas
Espionaje industrial	Ventaja competitiva Espionaje económico	Explotación económica Robo de información Intrusión en la privacidad Ingeniería social Penetración en sistemas Acceso no autorizado a sistemas
Insiders (disgustados, vagamente entrenados, malicia, negligencia, deshonestidad o empleados terminados)	Curiosidad Ego Inteligencia Beneficio monetario Venganza Errores u omisiones no intencionales	Asalto a empleados Chantaje Búsqueda de información propietaria Abuso computacional Fraude y robo Soborno Entrada de datos falsificados o corruptos Intercepción Código malicioso Venta de información Fallas en los sistemas Ingreso de intrusos en los sistemas Sabotaje de sistemas Acceso no autorizado a sistemas

Fuente: (Stoneburner,2002).

Se debe elaborar un documento de declaración de amenazas que se adapte a la organización y a su ambiente de procesamiento, en general la información de amenazas naturales debe estar fácilmente disponible. Las fuentes de información incluyen, pero no están limitados a agencias de inteligencia, centro de respuesta a incidentes computacionales y medios masivos, particularmente basados en recursos Web.

1.3 Identificación de vulnerabilidades

El análisis de las amenazas para sistemas de TIC debe incluir un análisis de sus vulnerabilidades. La meta de este paso es desarrollar una lista de las vulnerabilidades del sistema (los defectos o las debilidades) que podrían ser explotados por las amenazas potenciales.

Los métodos recomendados para identificar las vulnerabilidades de los sistemas son el uso de fuentes de vulnerabilidades, el rendimiento de las pruebas de seguridad en los sistemas, y el desarrollo de una lista de chequeo de requerimientos.

1.3.1 Fuentes de vulnerabilidades

Hoy día existen varias fuentes de información acerca de vulnerabilidades de los sistemas, Internet es una de las fuentes más poderosas, se puede encontrar información en páginas Web del fabricante, foros de discusión, listas de correo donde se intercambia las experiencias e incluso sitios Web especializados donde se publican las vulnerabilidades, como se explotan o se solucionan estas vulnerabilidades e información acerca de las personas o grupos que colaboraron en el descubrimiento. Las fuentes documentadas de vulnerabilidades que se deben considerar en el análisis de vulnerabilidades incluyen y no está limitado a:

- Documentación de valoraciones del riesgo previos.
- Reportes de auditorias a los sistemas TIC, reportes de sistemas anómalos, reportes de seguridad, y pruebas y evaluaciones realizadas en los sistemas.
- Listas de vulnerabilidades.
- Consejos de seguridad.
- Consejos de fabricantes.
- Listas Post y equipos comerciales de respuesta a incidentes.
- Alarmas y boletines de vulnerabilidad para asegurar la información de los sistemas militares.
- Análisis de seguridad de los sistemas de software.

1.3.2 Pruebas de seguridad en los sistemas

Se pueden ejecutar varias técnicas, métodos proactivos, empleo de pruebas, etc. para identificar las vulnerabilidades de los sistemas eficientemente, dependiendo de la criticidad y los recursos disponibles (Ej.: fondos, tecnología disponible, personas con la experticia para conducir estas pruebas, etc.).

En la actualidad existen herramientas automatizadas (comerciales, de fuente abierta, etc.) que pueden ser usados como fuentes de detección de vulnerabilidades, es posible

que estas herramientas arrojen falsos positivos y creen confusión, por eso debe existir en el equipo personal que conozca bien su infraestructura y sistemas para descartar estas posibilidades.

La evaluación y pruebas de los sistemas TIC es otra técnica que puede ser usada en el proceso de valoración del riesgo, esta incluye el desarrollo y la ejecución de protocolos de pruebas que comprueben la efectividad de los controles de seguridad de los sistemas de TIC como han sido aplicados en los ambientes operacionales. El objetivo es asegurarse que los controles aplicados cumplen las especificaciones aprobadas de seguridad para la implementación de software y hardware e implementan las políticas de seguridad de la organización o cumplen con los estándares de la industria.

Las pruebas de penetración pueden ser usadas para complementar la revisión de los controles de seguridad y asegurar las diversas facetas de los sistemas. Esta demuestra la capacidad de un sistema de soportar actos intencionales de violación de su seguridad.

1.3.3 Desarrollo de listas de requerimientos de seguridad

En este paso, el personal de la gerencia del riesgo determinará si los requerimientos de seguridad estipulados para el sistema de TIC y recolectados durante la caracterización de los sistemas son cumplidos por los controles existentes o planificados de seguridad, esta lista puede ser presentada en forma de tabla, con cada requerimiento acompañado de la explicación respectiva de cómo el diseño del sistema o la implementación cumple o no con los requerimientos de seguridad.

La lista de requerimientos de seguridad contiene los estándares de seguridad básicos que pueden ser usados para evaluar sistemáticamente e identificar las vulnerabilidades de los bienes (personal, hardware, software, información), procedimientos no automáticos, procesos, y transferencias de información asociadas con los sistemas de TIC en las siguientes áreas: administrativo, operacional, y técnico.

La salida de este proceso es la lista de requerimientos de seguridad, es importante tener en cuenta las regulaciones legales locales e internacionales para la elaboración

de esta lista. La Tabla 3 muestra los criterios sugeridos en la identificación de vulnerabilidades en cada una de las áreas:

Tabla 3. Criterios de Seguridad.

Área de Seguridad	Criterio de Seguridad
Administración Seguridad	Asignación de responsabilidades Continuidad de soporte Capacidad de respuesta a incidentes Revisión periódica de los controles de seguridad Separación de personal e investigaciones de fondo Valoración del riesgo Entrenamiento técnico y de seguridad Separación de funciones Autorización y reautorización de sistemas Plan de seguridad de aplicaciones o sistemas
Seguridad Operaciones	Control de agentes aéreos contaminantes Controles para asegurar la calidad de la fuente de energía Acceso y disposición de los medios de datos Etiquetado y distribución de datos externos Protección de las instalaciones Control de humedad Control de temperatura Seguridad de computadoras de escritorio, laptops.
Seguridad Técnica	Comunicaciones Criptografía Control de acceso discrecional Identificación y autenticación Detección de intrusos Reuso de objetos Auditoria de sistemas

Fuente: (Stoneburner,2002).

1.4 Análisis de Control

La meta de este paso es analizar los controles que han sido implementados o planeados para implementar por la organización para minimizar o eliminar la probabilidad que una amenaza se ejerza sobre un sistema vulnerable.

Para obtener una medida que indique la probabilidad que una vulnerabilidad potencial se pueda ejercer dentro del ambiente asociado a la amenaza (próximo paso), la implementación de los controles planificados o previstos debe ser considerada.

En los siguientes puntos se discuten algunos métodos, categorías de control y técnicas de análisis de control.

1.4.1 Métodos de control

Los controles de la seguridad abarcan el uso de métodos técnicos y no técnicos. Controles técnicos son las salvaguardas que se incorporan en el hardware, el software, o firmware. Controles no técnicos son administrativos y operacionales, como

políticas de seguridad, procedimientos operacionales, seguridad personal, física y ambiental.

1.4.2 Categorías de Control

Las categorías de control para los métodos técnico y no técnico pueden ser clasificados como preventivos o detectivos y se explican a continuación:

Los controles preventivos inhiben los intentos de violar la política de seguridad e incluyen controles tales como aplicación de controles de acceso, el cifrado, y autenticación.

Los controles detectivos advierten de intentos de violación de la política de seguridad e incluyen controles como rastros de auditoría, métodos de detección de intrusos, etc.

Posteriormente se explicarán estos controles desde el punto de la implementación. La cual durante el proceso de mitigación del riesgo es el resultado directo de la identificación de deficiencias en los controles actuales o planificados en el proceso de gerencia del riesgo.

1.4.3 Técnicas de análisis de control

Como se discutió en puntos anteriores, el desarrollo de listas de requerimientos de seguridad o el uso de listas de chequeo disponibles es de ayuda al analizar los controles de manera eficiente y sistemática. La lista de requerimientos de seguridad puede ser usada para validar el cumplimiento y no cumplimiento. Por lo tanto, es esencial actualizar esta lista para reflejar cambios en el entorno de los controles organizacionales y así asegurar la validez de dichas listas. Se tiene que la salida de este paso es la lista de los controles planificados a ser usados para mitigar la probabilidad de que se ejerza alguna amenaza sobre alguna vulnerabilidad existente y reducir el impacto de eventos adversos.

1.5 Determinar la probabilidad

Para derivar un grado total de probabilidad, se debe indicar la posibilidad que una vulnerabilidad se pueda ejercer potencialmente por amenazas asociadas a los siguientes factores:

- Motivación del origen de las amenazas y su capacidad.

- Naturaleza de las vulnerabilidades.
- Existencia y efectividad de los controles actuales.

Esta probabilidad se puede describir como alta, media, o baja. En la Tabla 4 se describen estos niveles de probabilidades. La salida de este proceso es la estimación de la probabilidad

Tabla 4. Definición de la probabilidad.

Nivel de Probabilidad	Definición
Alto	El origen de la amenaza esta altamente motivado y es suficientemente capaz, y los controles para prevenir que la vulnerabilidad se pueda ejercer son inefectivos
Medio	El origen de la amenaza esta motivado y es capaz, pero existen controles que tal vez impidan el ejercicio exitoso de la vulnerabilidad
Bajo	El origen de la amenaza carece de motivación o capacidad, o los controles existentes previenen o al menos impiden significativamente que la vulnerabilidad sea ejercida

Fuente: (Stoneburner,2002).

1.6 Análisis de impacto

El próximo paso en medir el nivel del riesgo es determinar el impacto resultado del ejercicio efectivo de alguna vulnerabilidad. Antes de empezar el análisis de impacto, es necesario obtener la siguiente información:

- Misión del sistema.
- Criticidad de los sistemas y datos.
- Sensibilidad de los sistemas y datos.

Esta información puede ser obtenida de la documentación existente de la organización. El análisis del impacto en la misión da prioridad a los niveles asociados con el compromiso de los bienes informáticos de la organización. La valoración de la criticidad identifica y asigna prioridad a los bienes informáticos críticos y sensibles de la organización, que soportan su misión crítica. La sensibilidad de los datos y sistemas también puede ser determinado (en caso de ausencia de documentación) basado en el nivel de protección requerida para mantener la CIA de los datos y sistemas, lo importante es relacionar a los propietarios de la información y sistemas que son los responsables en determinar el nivel de impacto.

Debido a la naturaleza genérica de la discusión, se designan los valores de impacto alto medio o bajo, la Tabla 5 muestra la descripción de las categorías y en la Tabla 6 se tiene el valor de la clase de impacto (cuantitativa).

Tabla 5. Valores de Impacto.

Magnitud del impacto	Definición del impacto
Alto	Puede resultar en alto costo por pérdida de bienes tangibles o recursos. Puede significativamente violar, dañar, o impedir la reputación, interés o misión de la organización. Puede resultar en muerte o daños serios.
Medio	Puede resultar en costos de bienes tangibles o recursos. Tal vez viole, dañe o impida la misión de la organización. Tal vez resulte en daño a seres humanos.
Bajo	Puede resultar en pérdida de algún bien tangible o recurso. Puede perceptiblemente afectar la misión, reputación o interés de la organización.

Fuente: (Stoneburner,2002).

Tabla 6. Valor de la clase de Impacto.

Clase de impacto	Valor de la clase de impacto
HBI (Alto)	10
MBI (Medio)	5
LBI (Bajo)	2

Fuente: (Stoneburner,2002).

1.7 Determinación del riesgo

1.7.1 Formular la prioridad del riesgo.

En este punto se debe determinar el nivel de riesgo de los bienes informáticos a fin de potenciar su prioridad, para el cual debe ser realizado un estudio cualitativo, cuantitativo o híbrido de ambos procedimientos. Esta perspectiva anterior es fuente de controversia y dependiendo del autor se describen ventajas y desventajas, siendo la ultima tendencia el empleo de procedimientos híbridos (Microsoft, 2006). Debido a que la Guía de Gerencia del Riesgo para los Sistemas de Tecnologías de Información de NIST (Stoneburner,2002) solo abarca el aspecto cualitativo del riesgo, en esta investigación se toma en consideración la Guía para la Gerencia del Riesgo de la Seguridad (Microsoft,2006) que es un híbrido cuantitativo y cualitativo.

Aspecto Cuantitativo

En la Gerencia del Riesgo Cuantitativo la meta es intentar calcular los valores numéricos para cada uno de los bienes informáticos recolectados durante la valoración del riesgo. Por ejemplo, se estima el valor verdadero de cada activo del negocio en términos de lo que costaría para reemplazarlo, de productividad perdida,

de reputación de marca de fábrica, y otros valores de negocio directo e indirecto. El esfuerzo es para utilizar la misma objetividad al computar la exposición del activo, el coste de controles, y todos los otros valores que se identifiquen durante el proceso de la gerencia de riesgo.

Existen algunas debilidades significativas inherentes en este acercamiento que no son fáciles de superar. Primero, no existe una vía formal o rigurosa para calcular efectivamente los valores para los bienes y sus controles. En otras palabras, mientras pareciera que da más detalles, los valores financieros restan importancia al hecho de que los números están basados en estimaciones. ¿Cómo se puede calcular precisa y exactamente el impacto que un incidente público de seguridad pudo tener en la organización? Segundo, las empresas que han tratado meticulosamente de aplicar todos los aspectos del riesgo cuantitativo han encontrado el proceso extremadamente costoso. Estos proyectos toman mucho tiempo en completar su primer ciclo, y usualmente involucran muchos miembros de personal argumentando acerca de valores fiscales específicos que fueron calculados. Tercero, las organizaciones con bienes de alto valor, el costo de exposición es tan alto que gastarían cantidades excesivas de dinero para mitigar los riesgos a los que son expuestos. Esto no es realista, las organizaciones no pueden gastar todo su presupuesto en proteger un bien simple, aunque sean los cinco más importantes.

Los ítems de entrada que provienen del análisis cuantitativo brindan metas y resultados claramente definidos. Los siguientes ítems generalmente son derivados de este análisis:

- Asignar valores monetarios a los bienes.
- Lista de las amenazas significativas.
- La probabilidad de ocurrencia de cada amenaza.
- La pérdida potencial de la compañía por amenazas en 12 meses (1 año).
- Salvaguardas recomendados, controles y acciones.

Aspecto Cualitativo

Lo que diferencia principalmente la valoración del riesgo cuantitativo del cualitativo, es que no se trata de asignar valores monetarios a los bienes, pérdidas esperadas, y

costos de control. Al contrario, se asignan valores relativos. Usualmente se hace una combinación de cuestionarios y mesas de trabajo involucrando personas de diferentes grupos en la organización como: expertos de seguridad, gerentes y equipos de tecnología, responsables de los bienes por parte del negocio y alta gerencia. Los cuestionarios son entregados días o semanas antes de los talleres, estos son diseñados para descubrir que bienes y controles están desarrollados, y que la información obtenida pueda ser de ayuda en los talleres siguientes. En los talleres los participantes identifican los bienes y asignan valores relativos. Luego se trata de saber que amenaza puede afectar a cada bien, y luego tratar de imaginar que tipos de vulnerabilidades estas amenazas podrían explotar en un futuro. Los expertos de seguridad de la información y los administradores de los sistemas conocen los controles que mitigan los riesgos y aproximan los costos de cada control. Finalmente, los resultados son presentados a la gerencia para su consideración en un análisis costo-beneficio.

Tabla 7. Ventajas y desventajas del Riesgo Cuantitativo y Cualitativo

	Cuantitativo	Cualitativo
Ventajas	Se asigna prioridad a los riesgos por su impacto financiero. Los resultados facilitan a la gerencia del riesgo retornando la inversión en seguridad. Los resultados pueden ser expresados en terminología específica de la gerencia. La exactitud tiende a incrementar en el tiempo así como la organización elabora registros históricos de los datos mientras gana experiencia.	Permite visibilidad y entendimiento de los niveles de riesgo. Fácilmente se llega a consenso. No es necesario cuantificar la frecuencia de las amenazas. No es necesario calcular los valores financieros de los bienes. Es fácil involucrar personal que no son expertos en seguridad de computación.
Desvent.	El valor del impacto asignado al riesgo es basado en valores subjetivos de los participantes. El proceso muestra resultados creíbles y consenso en largo tiempo. Los cálculos pueden ser complejos y consumir mucho tiempo. Los resultados son presentados en términos monetarios, y tal vez sea difícil para personal no técnico interpretarlo. El proceso requiere experiencia, los participantes no pueden ser entrenados tan fácilmente.	Diferenciación insuficiente entre los riesgos importantes. Difícil justificar las inversiones en la implementación de controles debido a que no existe una base para un análisis costo beneficio. Los resultados son dependientes de la calidad del equipo de gerencia del riesgo que se haya creado.

Fuente: (Microsoft,2006).

Comparación de la valoración del riesgo cualitativo y cuantitativo

Ambos métodos tienen sus ventajas y desventajas, ciertas situaciones hacen que las organizaciones adopten uno u otro. La Tabla 7 muestra un resumen de estas ventajas y desventajas.

El proceso de asignación de prioridades adiciona el elemento probabilístico a las declaraciones de impacto, en etapas anteriores se mostró como asignar la probabilidad al ejercicio de las amenazas y también como afectan estas a la organización. El resultado final es una lista con asignación de prioridades a los riesgos que son usados como entrada en el proceso de soporte de decisiones.

1.7.2 Completar la lista de niveles de riesgo

Luego de estimar la probabilidad de ejercicio de las amenazas y su impacto, el equipo de Gerencia del Riesgo Informático estima la probabilidad de los riesgos, dependiendo de ambos parámetros, luego usando la Tabla 8 se determina el nivel de riesgo de cada bien.

Tabla 8. Impacto y probabilidad.

		Summary Level Risk Rating		
Impact (from Impact Table above)	**High**	Moderate	High	High
	Med	Low	Moderate	High
	Low	Low	Low	Moderate
		Low	**Medium**	**High**
		Probability Value		

Fuente: (Microsoft,2006).

Cada organización puede modificar sus niveles de riesgo dependiendo de sus políticas de seguridad de la información. Con niveles de riesgo de la organización se puede elaborar la lista de estos, la Tabla 9 muestra un ejemplo:

Tabla 9. Listado de Niveles de Riesgo.

Information Collected During Data Gathering Process						
Asset				Exposure		
Date Identified	Asset Name	Asset Class	Applicable Defense-in-Depth Layer(s)	Threat Description	Vulnerability Description	Expo Rating
example	Consumer financial investment data	HBI	Host	Unauthorized access to consumer data through theft of Financial Advisor credentials	Theft of credentials off managed LAN client via outdated configuration of antivirus signatures, host configuration, or outdated security patches	
example	Consumer financial investment data	HBI	Host	Unauthorized access to consumer data through theft of Financial Advisor credentials	Theft of credentials off managed, remote client via outdated configuration of antivirus signatures, host configuration, or outdated security patches	M
exampla	Consumer financial investment data	HBI	Data	Unauthorized access to consumer data through theft of Financial Advisor credentials	Theft of credentials by trusted employee abuse via non-technical attacks, e.g. social engineering or eavsdropping	

scription	Exposure Rating (H,M,L)	Impact Rating (H,M,L)	Probability (H,M,L)	Summary Risk Level (H,M,L)
anaged LAN client ation of antivirus uration, or outdated tes	M	H	M	H
naged, remote ration of antivirus ation, or outdated ches	M	H	H	H
ed employee abuse cks, e.g. social vsdropping	L	M	L	L

Fuente: (Microsoft,2006).

1.7.3 Revisión con los "Stakeholders"

Una vez realizada la lista se debe revisar con el equipo de Gerencia del Riesgo Informático involucrando a los dueños de los bienes por el negocio. La meta es actualizar a los involucrados en el proceso de la valoración del riesgo y solicitar su opinión para ayudar en la selección de los riesgos que se estudiarán con un análisis detallado (cuantitativo).

1.7.4 Realizar Listado Detallado del Riesgo y asignar prioridades

La producción del Listado Detallado del Riesgo es la última y más importante actividad en el proceso de valoración del riesgo, porque permite a la organización entender los riesgos más importantes que la afectan. Una vez terminado el proceso de

valoración del riesgo, en algunos casos es suficiente enviar documentación de los riesgos a los "stakeholders" para iniciar acciones.

El listado detallado del riesgo obtiene sus entradas del Listado de Niveles de Riesgo realizado en puntos anteriores, sin embargo la lista detallada requiere que el equipo de Gerencia del Riesgo sea más específico en la descripción del impacto y su probabilidad. Para cada ítem en el Listado de Niveles de Riesgo se debe verificar cada combinación de amenazas y vulnerabilidades sea única a través de los riesgos.

El último elemento del Listado Detallado del Riesgo es un estimado cuantificado en términos monetarios. El estimado cuantitativo es determinado después de los valores del riesgo detallado, como se describe en las siguientes tareas:

1.7.5 Determinar impacto y exposición.

Es importante recordar que los riesgos incluidos en la revisión detallada son los clasificados como altos y medios dependiendo de la política que se involucre al respecto. Para empezar es necesaria la caracterización de los sistemas realizada en pasos anteriores, luego el valor de exposición de dichos bienes se da en un rango del 1 al 5, este valor se va a obtener dependiendo de cómo se afecta al negocio en la CIA.

Tabla 10. Valor de exposición de la confidencialidad e Integridad.

Valor de exposición	Compromiso de la Confidencialidad e Integridad
5	Daño severo o completo
4	Daño severo no completo
3	Daño moderado o pérdida
2	Daño bajo o pérdida
1	Cambios menores o sin cambios

Fuente: (Microsoft,2006).

La Tabla 10 muestra la escala de afectación en cuanto a la Confidencialidad e Integridad y luego la Tabla 11 describe la escala de afectación en relación a la disponibilidad. Luego el valor más alto de las 2 tablas que corresponde a cada ítem es el que se coloca como probabilidad de exposición.

En caso de existir dudas con respecto a los niveles de exposición puede ser factible programar reuniones con los propietarios por del negocio de estos bienes para aclarar cualquier duda.

Tabla 11. Valor de exposición de la disponibilidad.

Valor de exposición	Disponibilidad	Descripción
5	Parada de trabajo	Costos sustanciales de soporte o compromisos de negocios cancelados
4	Interrupción de trabajo	Incremento cuantificable de costos de soporte o compromisos de negocio retardados
3	Retardo de trabajo	Impacto considerable en los costos de soporte y productividad. No hay impacto medible en el negocio
2	Distracción del trabajo	No hay impacto medible, incrementos menores en soporte o infraestructura de costos
1	Absorbido por operaciones normales	No hay impacto medible para costos de soporte, productividad o compromisos de negocio

Fuente: (Microsoft,2006).

Una vez identificados los valores de exposición, se debe determinar el valor del impacto. En el proceso de Listado de Riesgo Detallado, el impacto es el producto del valor de la clase de impacto y el factor de exposición. A cada factor de exposición se le va a asignar un porcentaje como muestra la Tabla 12 que refleje el grado de daño al activo, este porcentaje es llamado el Factor de Exposición (EF). Cada valor de impacto es asociado con un valor cualitativo de alto, medio o bajo. Esta clasificación ayuda en comunicar el nivel de impacto y hacer seguimiento de los elementos de riesgo a través de cálculos detallados.

Tabla 12. Como se determinan los valores de impacto.

Valor Factor de Exposición	Factor de Exposición	Rango de Impacto	Nivel comparativo resumen
5	100%	7-10	Alto
4	80%	4-6	Medio
3	60%	0-3	Bajo
2	40%		
1	20%		

Fuente: (Microsoft,2006)

En la Tabla 13, se muestra un ejemplo de estos cálculos.

Tabla 13. Ejemplo de Valores de Clases de Impacto Detallado.

Activo		Exposición				
Nombre del Activo	Clase Imp.	Capa Defensa-en-profundidad	Descripción de la Amenaza	Descripción de la vulnerabilidad	Cal. Expo.	Cal. Imp.
Datos del consumidor de inversiones financieras	10 (HBI)	Host	Acceso no autorizado a datos del cliente a través de robo de las credenciales financieras	Robo de credenciales de clientes administrados LAN vía huellas no actualizadas de antivirus, configuración del equipo o parches fuera de fechas	4 (80%)	8
Datos del consumidor de inversiones financieras	10 (HBI)	Host	Acceso no autorizado a datos del cliente a través de robo de las credenciales financieras	Robo de credenciales de clientes remotos vía huellas no actualizadas de antivirus, configuración del equipo o parches fuera de fechas	4 (80%)	8

Fuente: (Microsoft,2006)

1.7.6 Identificar los controles actuales

Estos son los controles que reducen la probabilidad de ejercicio de una amenaza definido anteriormente. La medición efectiva de controles es evaluada en los cálculos probabilísticas detallados; sin embargo, documentar los controles aplicables apoya cuando se deben comunicar los elementos de riesgo. Es de mucha ayuda organizar las descripciones de los controles en categorías bien conocidas de gerencia, operaciones o grupos de control técnicos.

1.7.7 Determinar la probabilidad de impacto.

El valor de la probabilidad consiste en 2 factores. El primer valor determina la probabilidad que la vulnerabilidad exista basada en atributos de vulnerabilidades y posibles ataques. El segundo valor determina la probabilidad que la vulnerabilidad exista basada en la efectividad de los controles, cada valor es representado en un rango de 1-5.

La Tabla 14 muestra los valores dependientes de factores como:

Población del atacante (attacker population): La probabilidad de explotar alguna vulnerabilidad aumenta como aumenta la población del atacante en tamaño, así como sus habilidades.

Acceso Remoto Vs. Local: la probabilidad de explotar alguna vulnerabilidad aumenta si se realiza localmente.

Visibilidad del ataque (visibility exploit): la probabilidad normalmente incrementa si el ataque es bien conocido y publico.

Automatización del ataque. La probabilidad incrementa si el ataque puede ser programado para que busque automáticamente vulnerabilidades en grandes ambientes.

Es importante recordar que el cálculo de probabilidades de ataque es de naturaleza subjetiva.

Tabla 14. Evaluación de vulnerabilidades.

Definición de probabilidades por vulnerabilidad
Alta
Gran población atacante – "Script-Kiddie"/Hobbyist
Ejecutable remoto
Necesidad de privilegios anonimos
Métodos de explotación publicados externamente
Automatizados
"5" si aplica alguno
Medio
Población atacante media
Ejecutable no remoto
Niveles privilegiados de usuario requeridos
Métodos de explotación no públicos
No automatizados
"3" si aplica alguno
Bajo Población atacante pequeña – Conocimiento del intruso
Ejecutable no remoto
Niveles privilegiados de Administrador
Métodos de explotación no públicos
No automatizados
"1" si aplica alguno

Fuente: (Microsoft,2006).

Luego se selecciona el valor apropiado como muestra la Tabla 15.

Tabla 15. Evaluación del valor de la probabilidad.

Suma de vulnerabilidad	
Exposición de atributos (seleccionar uno)	
Alto	5
Medio	3
Bajo	1
Valor de la probabilidad (1,3, o 5)	

Fuente: (Microsoft,2006).

La Tabla 16 evalúa la efectividad de los controles. Como se mencionó anteriormente este es un valor de naturaleza subjetiva y se sustenta en la experiencia del equipo de análisis de riesgo para entender los controles.

Tabla 16. Evaluación de la efectividad de los controles.

¿Son efectivos los controles actuales?	
Si-0, No-1	
¿Es definida y aplicado efectivamente el "Accountability"?	1,0
¿Está comunicada y seguida efectivamente la concienciación?	1,0
¿Están definidos y practicados efectivamente los procesos?	1,0
¿Existen tecnologías o controles que reduzcan las amenazas efectivamente?	1,0
¿Son auditadas suficientemente las practicas actuales para detectar abuso o deficiencias de control?	1,0
Suma de atributos de control (0-5)=	

Fuente: (Microsoft,2006)

Una vez finalizada la evaluación de la efectividad de los controles la sumatoria de los atributos de control se introduce en el listado de nivel detallado.

1.7.8 Determinar el nivel detallado de riesgo.

El valor del riesgo se obtiene del producto entre el valor del impacto (con los valores evaluados del 1-10) y el de la probabilidad. Esto da como resultado un rango de valores del 0-100. La Tabla 17 muestra un ejemplo del contenido de la Lista Detallada de Riesgo.

Aplicando la misma lógica usada en el Resumen de Niveles de Riesgo, la Lista Detallada de Riesgos también puede ser comunicada en términos cualitativos de Alto, Medio y Bajo. De esta manera es posible sea más fácil la comunicación de los riesgos a la organización, la Tabla 18 muestra los rangos de los impactos cualitativos.

Tabla 17. Ejemplo de la Lista Detallada de Riesgo.

Baseline Risk (Current)									
Asset		Exposure							
Asset Name	Impact Class Rating	Defense-In-Depth Layer	Threat Description	Vulnerability Description	Exposure Rating (1-5)	Impact Rating (1-10)	Current Controls Description	Probability Rating w/Control (1-10)	Risk Rating w/Control (0-100)
Consumer financial investment data	10 (HBI)	Host	Unauthorized access to consumer data through theft of Financial Advisor credentials	Theft of credentials off managed **LAN client** via outdated configuration of antivirus signatures, host configuration, or outdated security patches	4 (80%)	8	**1.** Each Advisor limited to own accounts, thus exposure < 100%. **2.** Email notices to patch/update. **3.** Antivirus update and patches enforced on LAN every few hours - narrowing compromise of host during time window of exploit vs. patch.	Vulnerability: 5 Control: 1 Total = 6	**48**
Consumer financial investment data	10 (HBI)	Host	Unauthorized access to consumer data through theft of Financial Advisor credentials	Theft of credentials off managed **remote client** via outdated configuration of antivirus signatures, host configuration, or outdated security patches	4 (80%)	8	**1.** Each Advisor limited to own accounts, thus exposure < 100%. **2.** E-mail notices to patch/update. - No solution to ensure compliance outside of LAN connectivity.	Vulnerability: 5 Control: 5 Total = 10	**80**

Fuente: (Microsoft,2006).

Tabla 18. Ranking de Resumen Cualitativo.

Impact rating * Probability rating = Risk Level			
Impact Rating Ranges		*	**Probability Ranges**
High	10 -- 7		10 -- 7
Medium	6 -- 4		6 -- 3
Low	3 -- 0		3 -- 0

Impact												
H	10	0	10	20	30	40	50	60	70	80	90	100
	9	0	9	18	27	36	45	54	63	72	81	90
	8	0	8	16	24	32	40	48	56	64	72	80
	7	0	7	14	21	28	35	42	49	56	63	70
	6	0	6	12	18	24	30	36	42	48	54	60
M	5	0	5	10	15	20	25	30	35	40	45	50
	4	0	4	8	12	16	20	24	28	32	36	40
	3	0	3	6	9	12	15	18	21	24	27	30
	2	0	2	4	6	8	10	12	14	16	18	20
L	1	0	1	2	3	4	5	6	7	8	9	10
		0	1	2	3	4	5	6	7	8	9	10
		L				M						H
		Probability										

Overall Risk	Risk level
41-100	High
20-40	Medium
0-19	Low

Fuente: (Microsoft,2006).

1.7.9 Cuantificación del Riesgo.

Hasta ahora en la valoración del riesgo se ha usado el aspecto cualitativo, para identificar y asignar prioridad a los riesgos de manera rápida y eficiente. Sin embargo, cuando se seleccionan estrategias óptimas de mitigación del riesgo, las acciones se toman dependiendo de las estimaciones de costos monetarios, y esto requiere más tiempo y dedicación, por ello se seleccionan los riesgos más significativos.

Obviamente, las estimaciones monetarias son de ayuda cuando se comparan los costos de varias estrategias de mitigación de riesgo, pero debido a la naturaleza subjetiva de valorar los bienes intangibles no existe un algoritmo exacto de cuantificación de riesgo.

El aspecto cuantitativo que se describe a continuación usa la caracterización de los bienes y los niveles de exposición revisados anteriormente y se muestran las tareas involucradas en este método:

- Asignación de valores monetarios a los bienes.
- Asignar valores monetarios a cada riesgo.
- Calcular el valor de la expectativa de pérdida simple, conocida por sus siglas en inglés como SLE (Single Loss Expectancy).
- Determinar la rata de ocurrencia anualizada, conocida por sus siglas en inglés como ARO (Annualized Rate of Ocurrence).
- Determinar la expectativa de pérdida anualizada conocida por sus siglas en inglés como ALE (Annualized Loss Expectancy).

1.7.9.1 Asignación de valores monetarios a los bienes.

Una vez escogidos los bienes con mayor impacto para el negocio, se asignan valores monetarios para el valor tangible e intangible. Como referencia, se pueden usar las siguientes categorías en la estimación del impacto de costos para cada bien:

- Costo de reemplazo.
- Costo de mantenimiento.
- Costo de redundancia/disponibilidad.
- Costos de licenciamiento.

- Reputación de la organización.
- Productividad de la organización.
- Ingresos anuales.
- Ventaja competitiva.
- Eficiencia operativa interna.
- Cumplimiento con requerimientos legales.

Una vez estimados los costos por cada categoría, se totalizan los valores para determinar el estimado por cada bien. El resultado debe ser una lista con todos los bienes con su prioridad asignada y el estimado de su costo monetarios para la organización.

1.7.9.2 Asignar valores monetarios a cada riesgo

Después de determinar los valores monetarios de los bienes de la organización, se debe identificar y seleccionar el valor apropiado para cada riesgo. Esta es de la misma clase usada en la Lista Detallada de Riesgo.

Dependiendo de los valores monetarios de los bienes, se asignan valores monetarios a los riesgos, se puede llegar a consenso con la experiencia del equipo de Valoración del Riesgo o usar pautas de materiales para tener bases en la valoración del riesgo. Por ejemplo, si una compañía genera ingresos anuales aproximados de US$200 millones, y se aplica el 5% de las pautas materiales, los bienes clasificados de alto impacto se le asignan valores de US$10 millones al riesgo. Basados en la experiencia pasada de equipos de IT de esta compañía se seleccionaron valores de US$5 millones a los riesgos de mediano impacto y US$1 millón a los de bajo impacto.

1.7.9.3 Calcular el valor del SLE

Ahora se determina el grado de daño al bien, en porcentaje. Este porcentaje es llamado el factor de exposición (conocida como EF por sus siglas en inglés), el mismo nivel es usado en la Lista Detallada de Riesgo. Luego se multiplica el valor del bien por el factor de exposición (EF), este valor es conocido como el SLE. Para referencia la Tabla 19 muestra un ejemplo del cálculo en el aspecto cuantitativo simple.

Tabla 19. Cálculo del SLE.

Valor de alto impacto = M$		Calificación Exposición	Factor Exposición %
		5	100
Clase activo		4	80
Valor HBI	$M	3	60
Valor MBI	$M/2	2	40
Valro LBI	$M/4	1	20
Riesgo estimado= Valor clase activo * Factor Exposición %=SLE			

Fuente: (Microsoft,2006).

Un ejemplo ilustrativo se muestra en la Tabla 20 a continuación.

Tabla 20. Ejemplos de SLE.

Descripción Riesgo	Valor clase activo	Calificación Exposición	Valor Exposición	SLE
Riesgo Cliente LAN	$10	4	80%	$8
Riesgo Cliente Remoto	$10	4	80%	$8

Fuente: (Microsoft,2006).

1.7.9.4 Determinar el Índice Anual de Ocurrencia (ARO por sus siglas en inglés).

Una vez calculado la expectativa de pérdida simple (SLE), se incorpora la probabilidad para completar el estimado de riesgo monetario. Una tendencia común es estimar que tan frecuente puede ocurrir el riesgo en el futuro, esta estimación se puede anualizar. La Tabla 21 se puede usar como una guía para ayudar a identificar y comunicar el valor cuantitativo para determinar el ARO.

Tabla 21. Cuantificación del ARO.

Calificación cualitativa	Descripción	Rango ARO	Ejemplos Descriptivos
Alto	Probable	>=1	Impacta una o más veces por año
Medio	Probable	.99 a .33	Al menos una vez 1 - 3 años
Bajo	No Probable	<.33	Menos frecuente cada 3 años

Fuente: (Microsoft,2006).

El Grupo de Seguridad todavía debe seleccionar un valor para representar el ARO.

1.7.5 Determinar el Índice Anualizado de Pérdida

Para finalizar el aspecto cuantitativo, se calcula el producto entre el ARO y el SLE.

ALE=SLE*ARO

Al determinar el Índice Anualizado de Pérdida se representa el costo potencial del riesgo en términos anualizados. Es importante entender que si se materializa un riesgo, el impacto ocurra en toda la organización, por lo tanto probablemente el gasto que genere no cuadre en los costos anuales. La Tabla 22 señala un ejemplo de ALE.

Tabla 22. Ejemplo de ALE.

Descripción Riesgo	Valor Clase Activo	Calificación Exposición	Valor Exposicion	SLE	ARO	Estimado cuantitativo
Riesgo Cliente LAN	$10	4	80%	$8	0.5	$4
Riesgo Cliente Remoto	$10	4	80%	$8	1	$8

Fuente: (Microsoft,2006).

Mitigación del Riesgo

La mitigación del riesgo, involucra la evaluación e implementación de los controles apropiados y recomendados para reducir el riesgo documentado en pasos anteriores.

La erradicación total del riesgo es prácticamente imposible, es responsabilidad de la alta gerencia y los gerentes funcionales aplicar e implementar soluciones costo/efectivas apropiadas y reducir el riesgo de la organización a niveles aceptables, con el mínimo impacto adverso en los recursos y misión de la organización. En adelante se describirán las opciones de mitigación del riesgo, las estrategias de mitigación del riesgo, implementación de controles, categorías de control y el análisis costo-beneficio usado para justificar la implementación de los controles recomendados.

Opciones de mitigación del riesgo

La mitigación del riesgo es una metodología sistemática usada por la alta gerencia. Puede ser lograda a través de las siguientes opciones de mitigación de riesgo:

Asumir: aceptar el riesgo potencial y continuar operando el sistema de TIC o implantar controles para reducir el riesgo a un nivel aceptable.

Evitar: evitar el riesgo eliminando la causa y/o consecuencia.

Limitar: limitar el riesgo implantando controles que minimicen el impacto adverso que la amenaza puede ejercer en la vulnerabilidad.

Planificar: gestionar el riesgo desarrollando planes de mitigación que den prioridad, implementen y mantengan controles.

Investigar y reconocer: reducir los riesgos de pérdida entendiendo las vulnerabilidades o fallas e investigando controles que corrijan las vulnerabilidades.

Transferir: transferir el riesgo usando otras opciones que compensen la pérdida.

La misión y metas de la organización deben ser consideradas para la selección de estas opciones de mitigación. La mejor práctica es el uso de tecnologías de distintos vendedores de productos de seguridad.

Estrategia de Mitigación.

La Figura 8 se muestra algunos puntos de acción para la mitigación del riesgo:

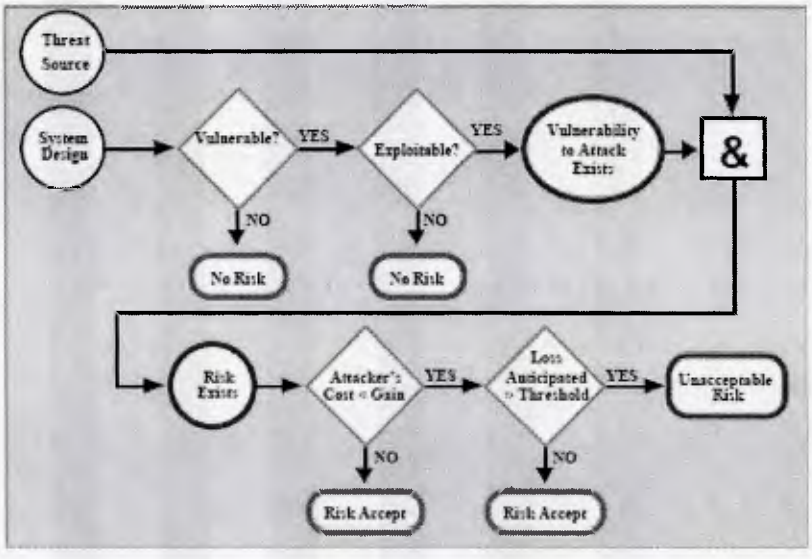

Figura 8. Puntos de Acción para Mitigación de Riesgo.

Fuente: (Microsoft,2006).

Esta estrategia se articula fondo en las reglas siguientes, que proporcionan la dirección en acciones para atenuar riesgos de amenazas humanas intencionales cuando:

- Una vulnerabilidad existe, se implementan técnicas que aseguren la reducción de la probabilidad que una vulnerabilidad pueda ser ejercida.
- Una vulnerabilidad puede ser ejercida, se debe aplicar protección por capas, diseños y arquitecturas de seguridad, y controles administrativos que minimicen el riesgo o prevengan la ocurrencia.
- El costo del atacante es menor que el riesgo potencial, se debe aplicar protección que reduzca la motivación del atacante e incremente su costo.
- Riesgo es demasiado grande, se deben aplicar principios de diseño, arquitecturas y protección técnica y no técnica que limite el grado de ataque, y consecuentemente reduzca la potencia de pérdida.

Implementación de Controles

Al aplicar acciones de control, las siguientes reglas se utilizan:

- Asignar prioridad a las acciones: usar la Lista de Riesgos Detallados para ubicar recursos, y situarlos a los de mayor prioridad, estos requieren acciones inmediatas correctivas para proteger los activos de la organización.
- Evaluar las opciones de control recomendados: puede que no sean las opciones más apropiadas y factibles para sistemas de TIC específicos de la organización. En este paso la factibilidad y efectividad de las opciones de control recomendados son analizados. El objetivo es escoger la opción de control más apropiada que minimice el riesgo.
- Realizar análisis costo-beneficio: para ayudar a la gerencia en la toma de decisión e identificar controles rentables, se realiza el análisis costo-beneficio, se describirá en detalle en pasos posteriores.
- Seleccionar el control: con base en los resultados del análisis costo-beneficio la gerencia determina el control más efectivo para reducir riesgos en la misión de la organización. La escogencia debe combinar elementos de control

técnico, operacional y administrativos que aseguren la seguridad adecuada para los sistemas de TIC de la organización.

- Asignar responsabilidades: las personas adecuadas quienes tengan la experticia apropiada y conjunto de habilidades para implementar los controles seleccionados son identificados y se asignan responsabilidades.
- Desarrollar plan de implementación: el plan como mínimo debe contener la siguiente información:
    - Riesgos y sus niveles asociados.
    - Controles recomendados
    - Acciones por prioridad.
    - Selección de controles planificados.
    - Recursos necesarios para implementar los controles seleccionados.
    - Lista de equipos responsables y sus miembros.
    - Fecha de inicio y fecha tentativa de finalización.
    - Requerimientos de mantenimiento.
    - Implementar los controles seleccionados: dependiendo de situaciones individuales identificar el riesgo residual.

La Figura 9 muestra el diagrama de la Metodología de Mitigación del Riesgo.

Categorías de Control

En la implementación de los controles recomendados para la mitigación del riesgo, la organización debe considerar controles técnicos, administrativos y seguridad en las operaciones o una combinación que maximice la efectividad de controles para los sistemas TIC de la organización.

Controles Técnicos de Seguridad.

Los controles técnicos de seguridad para la mitigación del riesgo pueden ser configurados para proteger de cierto tipo de amenazas. Estos pueden variar desde medidas simples hasta complejas y usualmente involucran arquitectura de sistemas; disciplinas de ingeniería; y paquetes de seguridad con una mezcla de hardware, software y firmware. Todas estas medidas deben trabajar juntas para asegurar datos

críticos y sensibles, información y funciones de sistemas TIC. Los controles técnicos son soporte, preventivos y detectivos.

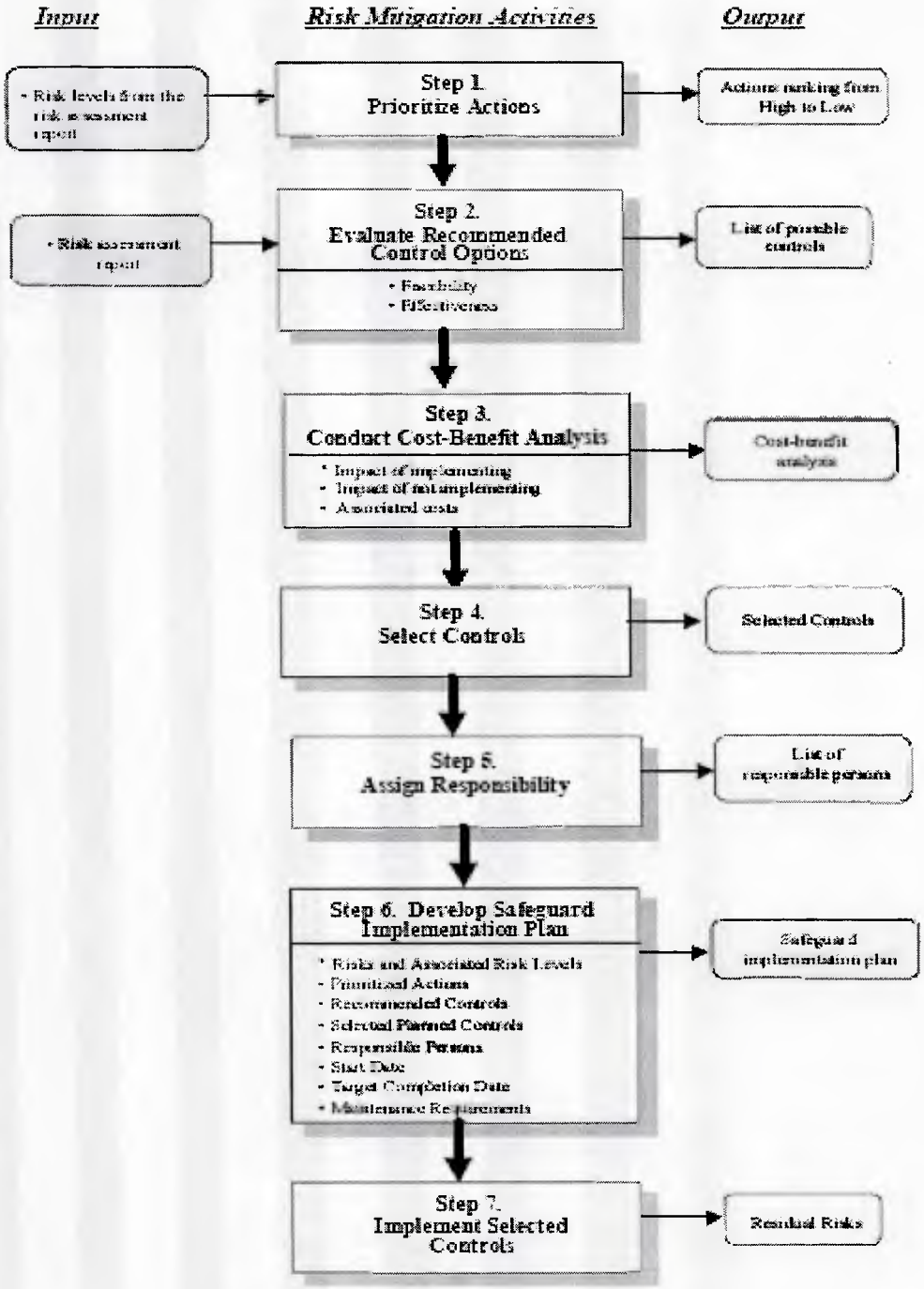

Figura 9. Metodología de Mitigación del Riesgo.

Fuente: (Microsoft,2006).

La Figura 10 muestra los controles de seguridad técnicos y sus relaciones entre ellos.

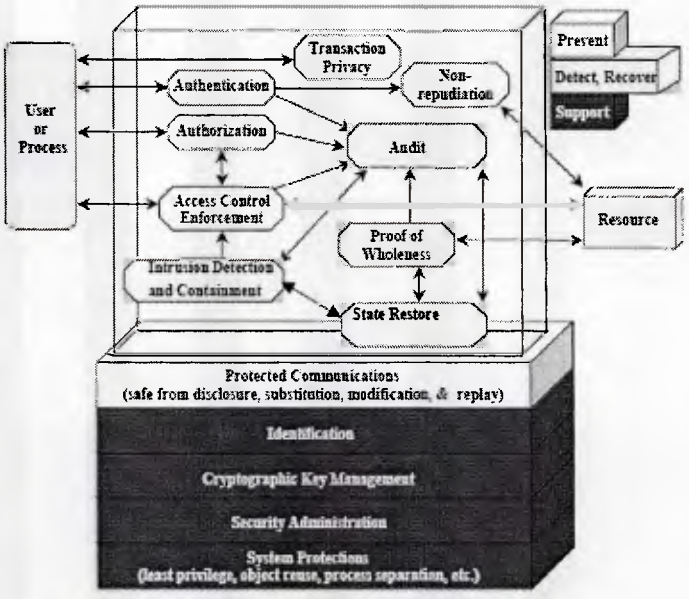

Figura 10. Controles Técnicos de Seguridad.

Fuente: (Microsoft,2006).

Controles Administrativos de Seguridad.

En conjunto con los controles técnicos y operacionales, son implementados para administrar y reducir el riesgo de pérdida y proteger la misión de la organización. Los Controles Administrativos se centran en la estipulación de políticas de protección de información, estándares y procedimientos llevados a cabo por procesos operacionales para cumplir las metas y la misión de la organización. Estos controles son preventivos, detectivos y de recuperación.

Controles Operacionales de Seguridad

Los estándares de seguridad de la organización deben establecer un conjunto de controles y lineamientos para asegurar que los procedimientos de seguridad que gobiernan el uso de los bienes y recursos de las TIC de la organización, y son llevados a cabo e implementados de acuerdo a las metas y misión de la organización. La gerencia juega un rol fundamental en hacer que se cumplan las políticas de

implementación y el aseguramiento que se establezcan los controles operacionales apropiados. Estos controles son preventivos y detectivos.

Análisis costo-beneficio

Para ubicar recursos e implementar controles costo-efectivos, las organizaciones, después de identificar todos los controles posibles y evaluar su factibilidad y efectividad, deben realizar un análisis costo-beneficio para cada controle propuesto y así determinar cuales son necesarios y apropiados para sus circunstancias.

Este análisis se presentó en el paso anterior 1.7.5. Los gerentes de la organización deben determinar que constituye un nivel aceptable para el riesgo de la organización. El impacto de los controles tal vez sea valorado, y el control incluido o excluido, después de que la organización determine el rango de niveles factibles. Este rango puede variar a lo largo de las organizaciones; sin embargo, las siguientes reglas aplican determinando el uso de nuevos controles:

- Si el control reduce el riesgo más de lo necesario, entonces se debe revisar cual es más o menos costoso.
- Si el control cuesta más que el beneficio de reducción de riesgo, entonces se debe encontrar otra cosa.
- Si el control no reduce el riesgo suficientemente, entonces se deben buscar otros controles.
- Si el riesgo provee suficiente reducción de riesgo y es costo-efectivo, entonces se usa.

Frecuentemente el costo de implementar un control es más tangible que el costo generado por un control nuevo o mejorado.

Riesgo Residual

Las organizaciones pueden analizar el grado de reducción del riesgo generado por los nuevos controles o los mejorados en términos de reducir la probabilidad de amenazas o el impacto, estos dos parámetros definen el nivel de mitigación del riesgo para la misión de la organización.

La implementación de los controles nuevos o mejorados puede mitigar el riesgo:

- Eliminando alguna de las vulnerabilidades de modo tal que reduzca el número de orígenes de amenazas/vulnerabilidades posibles.
- Agregue objetivos de control para reducir la capacidad y motivación del origen de las amenazas.

Reducir la magnitud del impacto adverso.

La relación entre la implementación del control y el riesgo residual se presenta en la Figura 11.

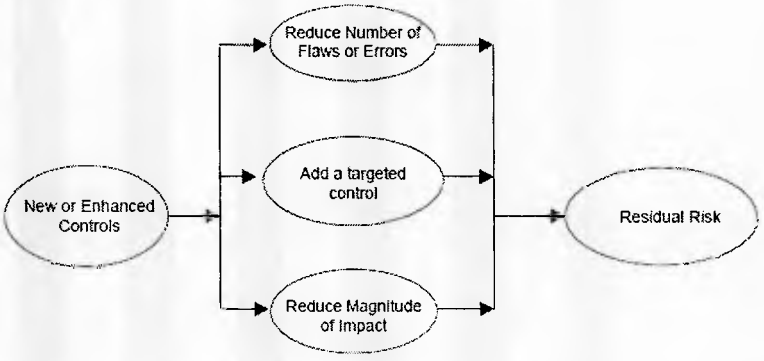

Figura 11. Implementación de controles y riesgo residual
Fuente: (Microsoft,2006).

El riesgo restante después de la implementación de controles nuevos o mejorados es el riesgo residual. Prácticamente no hay sistemas de TIC libre de riesgo, y no todos los controles implementados pueden eliminar el riesgo hasta cero.

Programa de evaluación de la efectividad.

En la mayoría de las organizaciones, las redes de TIC seguirán creciendo y expandiéndose, sus componentes cambiarán, y el software de la aplicaciones actualizándose o cambiándose a nuevas versiones. Además, el personal cambiará en el tiempo necesitando políticas de seguridad que cumplan con los requerimientos actuales. Estos cambios significan que nuevos riesgos estarán latentes y los riesgos previos mitigados se modifiquen y vuelvan a surgir de nuevo. Entonces, el proceso de gestión del riesgo siempre está en curso y constante evolución y desarrollo.

Después de la Gestión del Riego informático un factor clave en el ciclo de la seguridad es un programa efectivo de evaluación y valoración:

El proceso de Gestión del Riesgo se repite aproximadamente a cada 3 años. Deben existir calendarios específicos para valorar y mitigar los riesgos para la misión de la organización y hacerlos periódicamente flexibles para que se puedan implementar todos los cambios a los sistemas y ambientes de procesamiento de las TIC como resultado de nuevas tecnologías y políticas de seguridad. Las claves de éxito son:

- Compromiso de la alta gerencia.
- Soporte completo y participación del equipo de TIC.
- Competencia del equipo de valoración del riesgo.
- Concientización y cooperación de los usuarios.
- Evaluación y valoración del riesgo relacionado con las TIC.

Buenas Prácticas de Seguridad

Clasificación de la Información

Es claro que dependiendo del tipo de información que se este trabajando existe diferentes niveles de importancia para tratarla. Las organizaciones generalmente poseen datos importantes como "trade secrets", fórmulas o información de nuevos productos, si esta información se pierde o pasa a personas inescrupulosas se podría comprometer la confiabilidad de la empresa o causar vergüenza pública afectando la credibilidad y la imagen corporativa.

Por estas razones que se mencionan anteriormente, entre otras, es importante clasificar la información y garantizar cierto beneficio a la empresa.

Es probable que dependiendo de la clasificación que se asigne, se tomarán las medidas necesarias para garantizar la CIA de la información, no solo se debe proteger la información cuando la información sea útil, también es importante tomar los procedimientos necesarios para garantizar el desecho seguro de dicha información.

También la Clasificación de la Información sea necesaria para cumplir con reglamentos, leyes o cumplimiento corporativos que así lo requieran.

Beneficios de la Clasificación de la Información

- Demuestra el compromiso de la organización con la seguridad y protección.
- Ayuda a identificar que información es la más sensible o vital a la empresa.
- Soporta el postulado principal de la seguridad, CIA.
- Ayuda a identificar que protección aplica.

Clasificación

La clasificación mostrada a continuación coinciden usualmente con el sector gubernamental y militar (Krutz,2003):

No Clasificada (Unclassifed): información que se señala no sensible ni se clasifica. El lanzamiento público de esta información no viola secreto.

Sensible pero no clasificada (Sensible but unclassifed, SUB): información que ha sido designada como un secreto menor, no causará daños serios en caso de divulgación.

Confidencial (Confidential): información de naturaleza confidencial. El acceso desautorizado de esta información podría causar un cierto daño a la seguridad nacional.

Secreto (Secret): información de naturaleza secreta. La divulgación no autorizada puede causar serios daños a la seguridad nacional.

Secreto Superior (Top Secret): el más alto nivel en la clasificación. La divulgación no autorizada podría causar daños graves a la seguridad nacional.

Ahora se muestra a continuación la clasificación para el sector comercial:

Publico (Public): información similar a la no clasificada, cualquier información que no se ajuste a las clasificaciones que siguen pueden caer en esta categoría. En caso de ser divulgada no causará impacto adverso a la compañía.

Sensible (Sensitive): información que requiere un nivel mayor de clasificación que el público. Esta información se protege la confidencialidad e integridad.

Privado (Private): información considerada de naturaleza personal y prevista para uso interno exclusivamente. La divulgación no autorizada puede afectar en forma adversa a la compañía o a sus empleados.

Confidencial (Confidential): información considerar muy sensible y prevista para uso interno exclusivamente. Su divulgación no autorizada puede impactar seria y negativamente a la compañía.

Criterios

Algunos criterios para clasificar la información pueden ser:

- *Valor para el negocio*: grado de importancia para el negocio de la información, no solamente para el negocio sino también para la competencia.
- *Tiempo*: la clasificación de la información probablemente se reduzca a medida que pase el tiempo y tenga menor valor para el negocio.
- *Vida útil*: la información pierde valor por información nueva, cambios sustanciales en la compañía u otras razones.
- *Asociación de personal*: si la asociación es realizada personalmente o por leyes.
- Quién accederá los datos.
- Quién mantendrá los datos.
- Quién puede reproducir los datos.

Roles

Los roles para a tomar en cuenta para clasificar la información son (Krutz,2003):

Propietario: ejecutivo o gerente de la organización, es responsable por el bien que debe ser protegido. Tiene la responsabilidad final de protección de los datos siguiendo el concepto de "Due Care", tal vez sea obligado a proteger los datos en caso de alguna falla (por orden ya que la ejecución recae en el custodio). Sus responsabilidades son:

- Determinar que nivel de clasificación se va a asignar a la información basada en las necesidades del negocio para proteger los datos.
- Revisar las asignaciones de clasificación periódicamente y realizar las alteraciones que necesite como varíe el negocio.
- Delegar la responsabilidad del cuidado de los datos al custodio de la información.

Custodio: a este personal se le delega la responsabilidad por el propietario, este rol es comúnmente ejecutado por el personal de TIC. Las responsabilidades y tareas del custodio incluyen:

- Ejecutar backups regularmente y probar que funcionen adecuadamente.
- Ejecutar la restauración de datos de los respaldos cuando sea necesario.
- Mantener registros conservados de acuerdo con las políticas establecidas de Clasificación de la Información.

Usuario: cualquiera que en forma cotidiana use la información como parte de su trabajo. Algunos puntos importantes acerca de los usuarios:

- Deben seguir los procedimientos operacionales que define la política de Seguridad de la Organización.
- Deben tomar en cuenta el "Due Care" para preservar la información durante su trabajo.
- Deben usar los recursos para propósito de la organización exclusivamente.

Procedimiento

A continuación se indica uno de los procedimientos usados para clasificar la información según Fowler (2003):

- Identificar las fuentes de información.
- Especificar el criterio en como la información será clasificada y etiquetada.
- Clasificar los datos por su propietario, quien será sujeto a revisión por su supervisor.
- Especificar y documentar cualquier excepción a la política de clasificación.
- Especificar los controles que deben aplicar para cada nivel.
- Especificar los procedimientos de terminación para la desclasificación de la información o transferir la custodia de la información a otro ente.
- Crear programas de concientización acerca de los controles de clasificación.

Distribución

La distribución de la información se puede realizar por varias causas/vías:

- *Orden de la corte*: la información clasificada puede ser divulgada por orden de alguna corte.
- *Contratos gubernamentales*: algunos contratantes pueden divulgar información siguiendo los acuerdos de procura relacionados con proyectos del gobierno.
- *Aprobación de la alta gerencia*: la alta gerencia puede autorizar la divulgación de la información clasificada a organizaciones o entidades externas. Esta divulgación puede requerir acuerdos de confidencialidad entre las partes.

Concientización en Seguridad de la Información

La concientización de los usuarios en el tema de Seguridad de la Información puede que se tome a la ligera, en este caso el trabajo del personal de las TIC aumentará considerablemente y el manejo de la seguridad se hará más tedioso. Los usuarios deben internalizar la importancia de la protección tanto de su ambiente de trabajo como de la información que manipulan para lograr sus funciones, y este trabajo de concientizar debe estar en las políticas de seguridad de la organización.

Los controles y los procedimientos de un programa de seguridad deben reflejar la naturaleza de la información que se utiliza, y cada compañía tiene criterios propios para ello debido a su cultura.

Tipos de entrenamiento

Dependiendo del tipo de personal a entrenar existen diversos tipos de programas, generalmente existen 3 tipos de audiencias: gerentes, usuarios y empleados técnicos. Cada entrenamiento debe ser diseñado para la audiencia objetivo, las PEP deben ser explicadas a los gerentes para que las puedan aplicar de manera adecuada a sus colaboradores, y de este mismo modo debe existir otro programa para los colaboradores donde se explique a detalle la importancia, el que y como de las PEP, pero obviamente sin caer en detalles no relevantes, de igual manera sucede con el personal técnico.

Diversos tipos de material pueden ayudar en la tarea de concientización y entrenamiento:

- Presentaciones en vivo e interactivas, lecturas, videos y entrenamiento basado en computadoras (CBT)
- Distribución de publicaciones, posters, revistas, trípticos.
- Incentivos, premios, reconocimiento por logros.
- Recordatorios, mensajes en pantallas de acceso, protectores de pantalla, fondos de pantalla, Mouse pads, etc.

Rotación de trabajo

Para poder garantizar la operación de la organización y la independencia, lo cual es considerado una buena práctica, es importante que las personas que trabajan en el equipo puedan desempeñar cualquiera de las posiciones de sus compañeros y se dificulte la camaradería, así se minimiza el riesgo en caso de promoción, ausencia, despido, vacaciones, invalidez, muerte, etc.

Separación de funciones

La separación de funciones permite que una transacción u operación considerada importante no sea realizada totalmente por una sola persona, así se dificulta la posibilidad que se pueda llevar a cabo alguna actividad maliciosa. El incumplimiento de esta norma puede ocasionar hasta la revisión del contrato con el empleado.

Need to Know

Según Hansche (2004) se debe garantizar acceso a los usuarios solo a aquellos archivos y programas que ellos necesiten para ejecutar sus actividades asignadas. Es importante destacar que mientras se limite el acceso de los usuarios a ejecutar acciones que puedan elevar el riesgo de la seguridad, se pueden prevenir incidentes.

Practicas de contratación

En el inicio de una relación laboral es necesario realizar una revisión detallada a la hoja de vida del personal a contratar, si es necesario dependiendo del cargo verificar toda la información suministrada, realizar perfiles psicológicos e incluso pruebas de drogas. El punto importante es contar con personal altamente calificado, que se pueda predecir por la investigación de su pasado no tenga antecedentes criminales, este

personal puede que maneje información considerada importante para la organización y no se quiere poner en riesgo la seguridad. Incluso puede ser posible firmar acuerdos de confidencialidad, con declaraciones claras acerca de las consecuencias de incurrir en faltas.

Terminación

La finalización de la relación laboral puede darse por varias causas, es importante contar con procedimientos claros al respecto, ya que en el momento de ejecutar una finalización de la relación abrupta y no amistosa es necesario contar con el procedimiento claro en cuanto al manejo de personal y de los bienes que este posee pertenecientes a la compañía. Es probable que este procedimiento involucre personal perteneciente a seguridad física (vigilantes, guardias, etc.) que ayuden en la ejecución de los procedimientos.

Due Care

Las organizaciones que se preocupan en el desarrollo de políticas, estándares y procedimientos practican el "Due Care", son responsables por las actividades que se realizan en la corporación y toman los pasos necesarios para ayudar a proteger los empleados y los recursos de posibles riesgos.

Due Diligence

Es el acto de investigar y entender los riesgos que la compañía enfrenta.

Seguridad en el Desarrollo de Sistemas y Aplicaciones

El desarrollo de aplicaciones informáticas se pensó para facilitar y agilizar a los seres humanos el trabajo diario, ayudando a ejecutar sus labores en forma rápida y eficiente, dando la oportunidad a las masas de obtener resultados para satisfacer el aumento de requerimientos en todo el globo, fortaleciendo la productividad y generando tiempo que puede usarse en otros oficios.

Apoyado siempre en la tecnología, las soluciones informáticas se crearon como una herramienta de trabajo; inicialmente no se pensaba en seguridad de la información, pero con el transcurso de los años y a la par el auge de los delitos informáticos, se

volvió imperativa en el desarrollo de aplicaciones. A continuación se presenta algunos tópicos importantes de seguridad en el desarrollo de sistemas y aplicaciones para el conocimiento del lector.

Ciclo de Vida del Desarrollo de Software

La definición de ingeniería es la aplicación de la ciencia y matemáticas para el diseño y construcción de herramientas útiles para el hombre. La definición de software consiste en la suma total de los programas de cómputo, procedimientos, reglas de documentación y datos asociados que forman parte de las operaciones de un sistema de cómputo (IEEE,1993). Con lo cual, la ingeniería de software puede ser definida como la ciencia y arte de especificar, diseñar, implementar y desarrollar programas, documentación y procedimientos operativos para que las computadoras puedan ser útiles a los hombres. Esta definición es la combinación de definiciones populares de ingeniería y software.

En ingeniería de software, el termino verificación es definido como el proceso de establecer la correspondencia entre el producto de software y su especificación. Validación establece la aptitud o el valor de un producto de software para su misión operacional. Requerimientos, como se define en el modelo de cascada según Winston Roice (1970) (Waterfall Model), son la validación completa de las especificaciones de las funciones requeridas, interfaces y rendimiento para el producto de software. Producto es el diseño completo, especificaciones verificadas de toda la arquitectura de software-hardware, estructuras de control y estructuras de datos para el producto.

Software de calidad es difícil de obtener sin un proceso de desarrollo. Como en cualquier proyecto, dos metas principales del desarrollo de software son producir un producto de calidad que cumpla los requerimientos del cliente estando en el presupuesto y tiempos acordados. Una sucesión de modelos han emergido a través del tiempo incorporando mejoras en el proceso de desarrollo. El Modelo Inicial fue definido con etapas exitosas, tomando en cuenta que diferentes equipos y planificación son requeridos para cada etapa, fue muy simplista asumiendo que cada paso podía ser completado y finalizado sin tener efecto en las etapas posteriores que necesariamente requerían re-trabajo.

El modelo Cascada

Debido a que las etapas posteriores como diseño, codificación, y pruebas en el proceso de desarrollo pueden requerir modificar las etapas anteriores del modelo, emerge el modelo de Cascada (Royce,1970). En este, el desarrollo de software puede ser manejado si los desarrolladores están limitados en regresar solo una etapa anterior para hacer de nuevo el trabajo. Si esta limitación no es impuesta, entonces los desarrolladores pueden trabajar en cualquier fase en cualquier momento que lo requieran, derivándose en falta de control y dificultad en el manejo. El modelo en Cascada se muestra en la Figura 12.

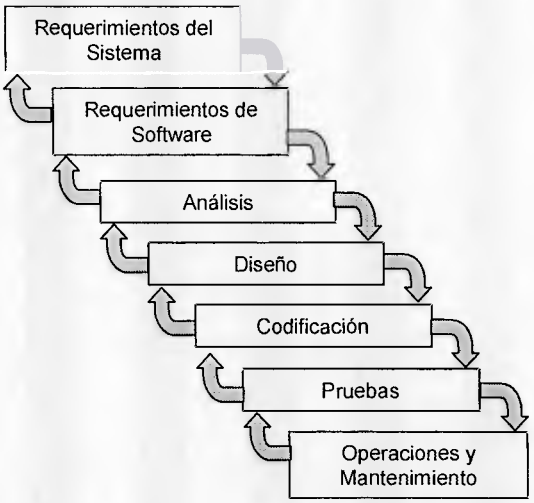

Figura 12. Modelo Cascada.
Fuente: (Royce,1970).

Un problema fundamental con estos modelos es que asumen que una fase o etapa finaliza en un momento específico; sin embargo, esto no es usual en aplicaciones del mundo real. Si en una fase final se fuerza trabajar por etapas, la situación puede ser mejorada. Si es necesario re-trabajo en este modo, la fase no se pronuncia como finalizada. El re-trabajo debe realizarse y las etapas del proyecto cumplidas antes de reconocer la fase oficialmente completa. En 1976, Barry Boehm reinterpreto el modelo en Cascada teniendo consigo fases y etapas del proyecto, incluyendo flechas

hacia atrás representando referencias anteriores para verificación y validación contra las líneas base definidas (ver Figura 13).

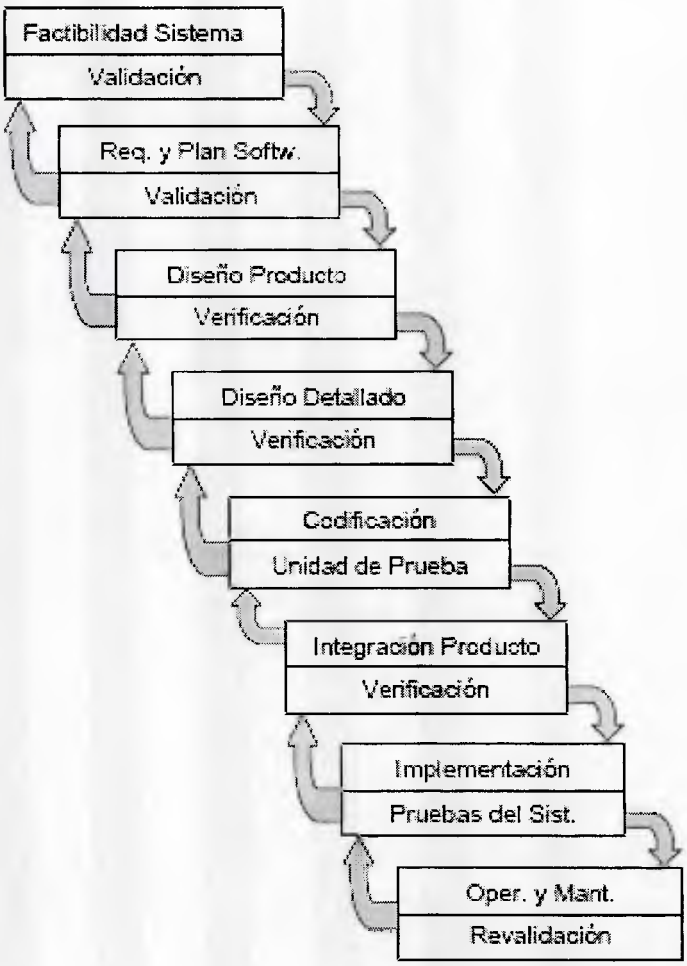

Figura 13. Modelo Cascada Modificado con Validación y Verificación.
Fuente: Krutz (2003) citando a Boehm (1976).

En esta versión modificada del modelo de Cascada, el final de cada fase es un punto en el tiempo para el cual no se necesitan fases de iteración provistas. El re-trabajo puede ser cumplido dentro de cada fase, cuando la fase finalice es requerido revisar las muestras.

Modelo Espiral

En 1988 en TRW, Barry Boehm desarrolló el modelo Espiral, que es de hecho un meta-modelo que incorpora un número de modelos de desarrollo de software, representa un espiral que incorpora varias fases del proceso. Como se muestra en la Figura 14, la dimensión angular representa el progreso realizado en completar la fase, y la dimensión radial representa el costo acumulado del proyecto. El modelo establece que cada ciclo del espiral envuelve la misma serie de pasos para cada parte del proyecto.

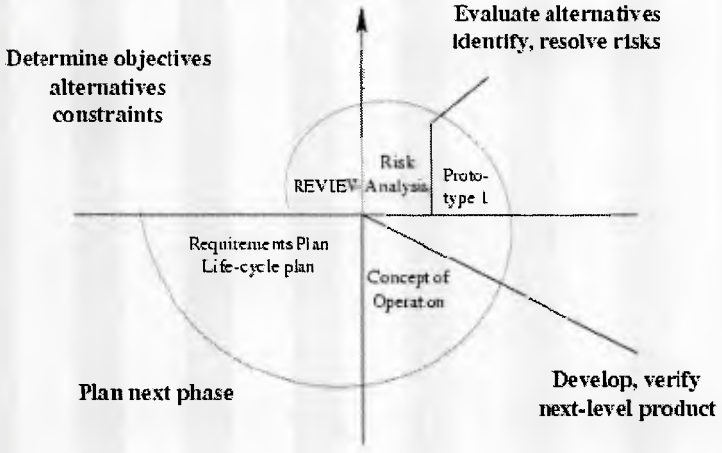

Figura 14. Modelo Espiral.
Fuente: Krutz (2003) citando a Boehm (1988)

El cuadrante inferior izquierdo se enfoca en planes de desarrollo que serán revisados en cuadrantes superiores del diagrama previo a la finalización de los planes. Entonces, después de tomar una decisión de continuar, el espiral se inicia en el cuadrante superior izquierdo. Este cuadrante en particular define los objetivos de parte del proyecto, significados de alternativas para cumplir parte del proyecto y las restricciones asociadas con estas alternativas.

Los próximos pasos involucrados en la evaluación de alternativas son respecto a los objetivos y restricciones del proyecto. Esta evaluación puede incluir prototipos, modelación y simulación. El propósito de este paso es identificar y evaluar los riesgos involucrados, y es mostrado en la parte superior derecha del modelo. Una vez

resueltos estos asuntos, el próximo paso en el procedimiento sigue el modelo de ciclo de vida tradicional. El cuadrante inferior derecho del espiral representa la fase de desarrollo final para cada parte del producto. Un concepto importante del modelo espiral es que el eje horizontal representa la revisión mayor que es requerida para completar el ciclo completo.

Progresivamente se han ido desarrollando modelos para el desarrollo de software y también la estimación del costo, un ejemplo de estos es el COCOMO que inicialmente diseño Barry Boehm en (1981) para estimar los costos de proyectos de desarrollo de software. Este modelo estimaba el esfuerzo de desarrollo de software y los costos como una función del tamaño del producto de software en el código origen. Ha sido modificado en varias oportunidades, mejorándolo e incluyendo nuevas variables que inciden en los costos de desarrollo de software.

También se pueden mencionar modelos como Medida de Función de Punto (SF), Curva Raileigh (SF); un modelo prominente que uso este método de estimación fue el modelo de Ciclo de Vida del Software. En él, las estimaciones son basadas en un número de líneas de código fuente modificadas por dos factores: el índice "Manpower buildup" (MBI), que estima el promedio de codificación de un equipo en el proyecto y el factor de productividad (PF), que esta basado en la tecnología usada.

Seguridad de la Información y el Modelo de Ciclo de Vida

En la mayoría de las prácticas de ingeniería y desarrollo de software, mientras más temprano se introduce un componente en un proceso, es más probable que sea exitoso, el costo sea menor y se disminuya el re-trabajo. En seguridad de la información esta no es la excepción, la concepción, desarrollo, implementación, pruebas y mantenimiento de controles deben ser realizadas concurrentemente con las fases del ciclo de vida de un sistema de software. Un acercamiento conceptual se puede ver en la Figura 15.

Pruebas

Las pruebas en los módulos de software o unidades de prueba deben ser realizadas cuando estos son diseñados. Personal aparte de los programadores son los indicados

para estas pruebas. Los datos de prueba son parte de las especificaciones para ellas. Las pruebas no deben incluir solamente datos válidos en los módulos, sino también tipos incorrectos, valores fuera de rango, y otras condiciones de borde. Guías especiales de prueba que incluyan todos los caminos de software en una extensión completa con resultados correctos deben ser conocidos antes de su uso.

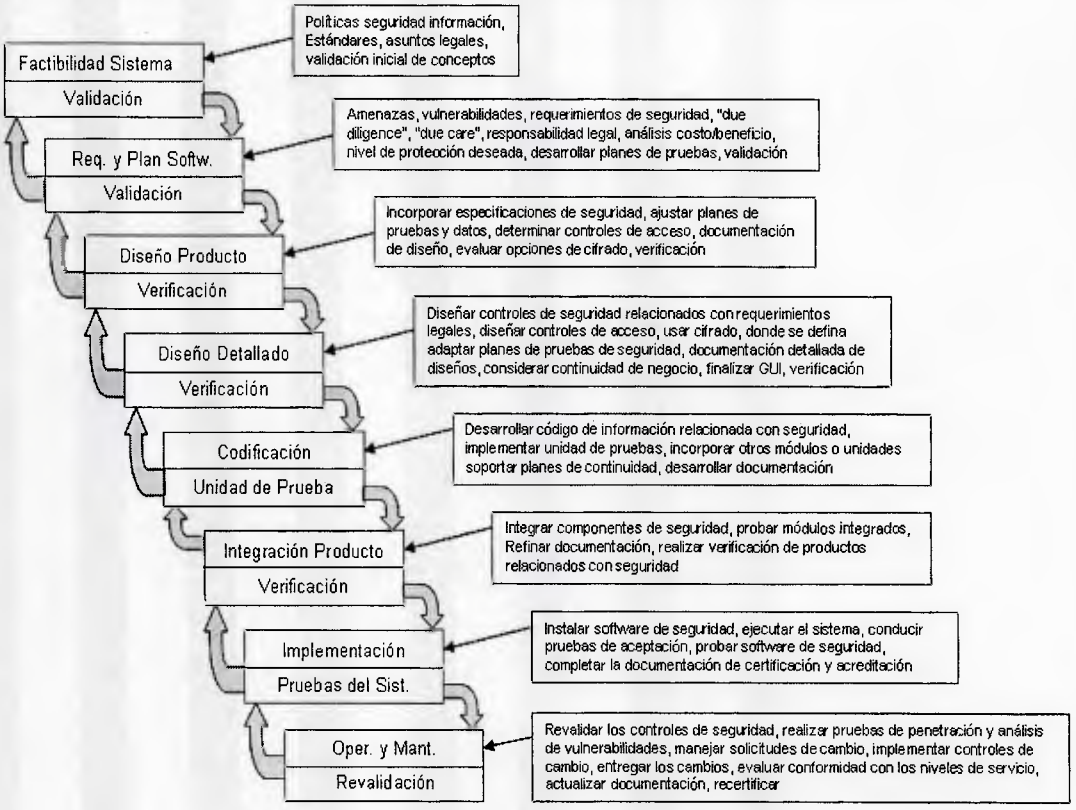

Figura 15. Componentes Seguridad Ciclo de Vida de Software.
Fuente: (Krutz,2003).

Consideraciones de Seguridad en el Ciclo de Desarrollo de Sistemas de Información

Para NIST (Grance,2004) se puede seguir una serie de pasos para integrar seguridad en el Ciclo de Vida de Desarrollo de Sistemas de Información (SDLC). Se explicará al lector en forma general de los aspectos cubiertos por NIST para lograr seguridad y cualquier información adicional se puede ver la guía publicada.

Tabla 23. Seguridad de TI en SDLC.

	Iniciación	Adquisición Desarrollo	Implementación	Operaciones Mantenimiento	Disposición
SDLC	Necesita determinar: Percepción necesidad Enlace de la necesidad con misión y objetivos de rendimiento Valoración de alternativas con bienes capitales Preparar para revisión de inversiones y presupuesto	Declaración funcional de la necesidad Investigación de mercado Estudio de factibilidad Análisis de alternativas Análisis costo beneficio Estudio de conversión de software Análisis de costo Plan gerencia del riesgo Plan de adquisición	Instalación Inspección Pruebas de aceptación Entrenamiento inicial de usuarios Documentación	Medición del rendimiento Modificación del contrato Operaciones Mantenimiento	Eliminación apropiada Intercambio y venta Proyección organización interna Transferencia y donación Cierre contrato
Consideraciones Seguridad	Categorización Seguridad Evaluación del riesgo preliminar	Valoración riesgo Análisis de requerimientos funcionales de seguridad Análisis de requerimientos asegurar seguridad Consideraciones costos y reporte Planificación seguridad Desarrollo de controles de seguridad Desarrollo de pruebas de seguridad y evaluaciones Otros componentes de planificación	Inspección y aceptación Integración de sistemas Certificación de Seguridad Acreditación de seguridad	Control y administración configuración Monitoreo continuo	Preservación de la información Sanidad del medio

Fuente: (Grance,2004)

En la Tabla 23 se muestra los ajustes de seguridad realizados en el SDLC. Estos pasos definen un marco conceptual para el planeamiento de la seguridad durante el SDLC. Este marco se debe utilizar solamente como ejemplo, no como metodología definitiva, contiene la descripción y consideraciones del planeamiento que conducirán a la producción de las especificaciones para la adquisición en seguridad de la información. Las organizaciones pueden utilizar otras metodologías o modificar la presentada aquí.

Sistemas de Base de Datos

Un sistema de base de datos puede ser usado como mecanismo general para definir, almacenar y manipular datos sin escribir programas específicos para ejecutar estas funciones. Un sistema manejador de bases de datos (SMBD) proporciona comandos

de alto nivel para operar en los datos de la BD. Existen diferentes tipos de bases de datos en las que se destacan:

- Jerárquicas
- Mesh – Acoplamiento
- Orientadas a objeto
- Relacionales

Seguridad en las Bases de Datos

En una BD relacional, la seguridad puede ser proporcionada a través del uso de vistas. Una vista es una relación virtual que combina la información de otras operaciones. Una vista puede ser usada para restringir los datos disponibles a los usuarios basados en sus privilegios y "mínimo privilegio". Una vulnerabilidad en la seguridad de las BD puede ser explotada a través de los SMBD. Diseñados para facilitar las consultas a la BD, el SMBD puede ser una fuente posible de compromiso de datos evitando los controles de seguridad normales. La granularidad de acceso a los objetos en una BD se refiere a la "fineza" en que estos accesos pueden ser controlados o limitados. Otros problemas de seguridad en las BD son la agregación y la inferencia. La agregación es el acto de obtener información de alta sensibilidad combinando información de bajo nivel de sensibilidad. La inferencia es la habilidad de los usuarios para deducir información acerca de datos en niveles sensibles para los cuales no tienen privilegios de acceso. Un enlace que permite que ocurra inferencia es llamado un canal de inferencia.

Control de aplicaciones

Una meta del control de aplicaciones es hacer cumplir las políticas de seguridad de la información de las organizaciones y procedimientos para mantener la CIA. La seguridad de las aplicaciones involucra la entrada al sistema, los datos a ser procesados y las salidas del sistema. Los controles pueden ser clasificados en medidas preventivas, detectivas y correctivas que aplican a diferentes categorías de seguridad. Los controles y categorías están listados en la Tabla 24.

Los usuarios que ejecutan aplicaciones requieren la disponibilidad del sistema. Un SLA garantiza la calidad del servicio al suscriptor por el proveedor de servicios de red. Niveles de servicios definidos son las bases para medir los servicios entregados y son de ayuda en anticipar, identificar y corregir problemas.

Tabla 24. Tipos de control de aplicaciones

Tipo de control de Aplicación	Precisión	Seguridad	Consistencia
Preventivo	Chequeo de datos, formas, pantallas, chequeos de validación, planes de contingencia, y backups	Firewalls, monitores de referenciales, etiquetas de sensibilidad, cifrado, clasificación de datos, one-time passwords, plan de contingencia, separación de funciones desarrollo, ambientes de aplicación y pruebas	Diccionario de datos, estándares de programación, y sistemas de administración de BD
Detectivos	Chequeo de redundancia cíclica, caminatas de revisión, hash, y chequeos razonables	Sistemas de detección de intrusos y registros de auditoría	Comparación de controles, pruebas de relaciones, y reconciliación de controles
Correctivos	Backups, reportes de control, antes/después reporte de imágenes, y reinicio de puntos de chequeo	Respuesta de emergencias y monitores de referencia	Comentar programas y controles de BD

Fuente: (Grance,2004)

Para aplicaciones seguras de acuerdo a (OWASP,2005), los requerimientos mínimos son los que se listan a continuación:

- Gerencia organizacional con un encargado de la seguridad de la información.
- Política de Seguridad de la Información escrita derivada apropiadamente de estándares y mejores prácticas nacionales e internacionales.
- Metodología de desarrollo con actividades y puntos de chequeo adecuados.
- Liberación de software con consideraciones de seguridad y administración de la configuración.

Requerimientos de Seguridad

Antes de poder determinar si una aplicación es segura, es necesario establecer cuales son sus requerimientos de seguridad. Para ello existe un estándar internacional para identificar y definir los requerimientos de seguridad que son de ayuda para muchas circunstancias: el estándar internacional ISO/IEC 15408:1999 (ISO/IEC15408,1998) mejor conocido como Common Criteria (CC). El CC es la culminación de décadas de trabajo para identificar requerimientos de seguridad en las tecnologías de información y comunicaciones.

El nombre oficial del CC es "Criterios Comunes para la Evaluación de Seguridad de la Tecnología de la Información".

A continuación se muestra información de carácter general sobre el CC para entender como aplicar sus conceptos. El documento tiene tres partes: la introducción, los requerimientos funcionales de seguridad y requerimientos para asegurar la seguridad, también existen otros documentos que dirigen a los evaluadores como aplicar el CC según la metodología para hacer evaluaciones formales (en caso de certificación).

Aunque puede ser utilizado en otras maneras, el CC se utiliza típicamente para crear dos clases de los documentos, el "Perfil de la Protección" (PP) o el "Blanco de la Seguridad" por sus siglas en ingles "security target" (ST). Un "Perfil de la Protección" (PP) es un documento creado por el grupo de usuarios que identifica las características deseadas de la seguridad de un producto. Básicamente, los PP son una lista de los requisitos de la seguridad del usuario, descrita en una manera muy específica definida por el CC. Un "Blanco de la Seguridad" (ST) es un documento que identifica lo que hace un producto realmente, o un subconjunto de ella, que sea relevante a seguridad. Un ST no necesita resolver los requisitos de ninguna PP particular, sino que un ST podría resolver los requisitos de unos o más PP (Wheeler,2003).

El PP y el ST pueden pasar por una evaluación formal. La evaluación de los PP simplemente asegura que resuelvan las reglas de documentación y chequeos de sanidad. Una evaluación del ST implica además de revisar el documento evaluar el sistema real (llamado el "blanco de la evaluación"). El propósito de una evaluación del ST es asegurarse que, el nivel de los requisitos del aseguramiento especificados por el ST y el producto real resuelven los requisitos funcionales de la seguridad. Los clientes pueden entonces comparar el ST evaluado con el PP qué desean. Con esta comparación, los consumidores pueden determinarse si los productos resuelven sus requisitos y en caso contrario, donde están las limitaciones.

Metodología de Desarrollo

Las casas de desarrollo de Software escogen metodologías y estándares de codificación. Desarrollos "Ad Hoc" no son estructurados para producir aplicaciones

seguras. Las organizaciones que deseen producir código seguro necesitan tener una metodología que soporta esta meta. Los atributos importantes cuando se escoge una metodología de desarrollo segura son:

- Aceptación consistente de diseño, pruebas y documentación.
- Puntos de chequeo donde los controles de seguridad sean adecuados.
- Funcione para el tamaño de la organización y su madurez.
- Tenga el potencial de reducir la tasa de error y mejorar la productividad de los desarrolladores.

Estándares de Codificación

Las metodologías no son estándares de codificación, cada organización debe determinar que debe usar basado en prácticas comunes o simplemente en mejores practicas. Se debe considerar:

- Arquitectura
- Niveles mínimos de documentación requeridos.
- Requerimientos de documentación mínimos.
- Requerimientos de pruebas mandatarios.
- Niveles mínimos de comentarios en la codificación
- Usar manejo de excepciones.
- Uso de controles de flujo.
- Métodos de asignación de nombres para variables, funciones, clases y tablas.
- Codificación que sea preferiblemente legible y fácil de mantener sobre códigos complejos.
- Identificación y tabulación normadas.

Control del código fuente

La ingeniería de software requiere el uso de mejoras regulares al código como de mecanismos de prueba asociados. Todos los códigos y pruebas deben ser capaces de reversar o asignar versión.

Criptografía

La criptografía abarca los principios, significados y métodos para enmascarar la información. Se debe hacer hincapié en los conceptos básicos de criptografía, algoritmos de claves públicas y privadas en termino de sus aplicaciones y uso; distribución de claves y su manejo, métodos de ataque y aplicaciones, construcción y uso de firmas digitales para proveer autenticidad electrónica de transacciones y no repudiación de las partes involucradas. Este tema tiene amplia información disponible en otros trabajos de investigación motivo por el cual no se abarcará en este trabajo.

Modelos y arquitecturas de seguridad

Este tópico incluye los conceptos, principios, estructuras y estándares usados para diseñar, implementar, monitorear y asegurar sistemas operativos, equipos, redes, aplicaciones y controles usados para asegurar niveles de confidencialidad, integridad y disponibilidad.

Se debe asegurar el conocimiento de los modelos de seguridad en términos de confidencialidad, integridad, flujo de información, requerimientos comerciales Vs. gubernamentales, modelos de sistemas en términos de las mejores prácticas como Common Criteria; plataformas técnicas en términos de hardware, firmware y software, técnicas de sistemas de seguridad en términos de controles preventivos, detectivos y correctivos. Este tema tiene amplia información disponible en otros trabajos de investigación motivo por el cual no se abarcará en este trabajo.

Seguridad de Operaciones

Es usada para identificar los controles en el hardware, medios y operadores con privilegios de acceso a cualquiera de estos recursos. La auditoria y el monitoreo son los mecanismos y herramientas que permiten la identificación de eventos de seguridad y reportarlos a individuos, grupos o procesos apropiados que tomen las medidas pertinentes.

Se deben conocer los recursos a ser protegidos, los privilegios a ser restringidos, los mecanismos de control disponibles, el abuso potencial de estos accesos, los controles apropiados y los principios de buenas prácticas que garanticen la segregación y rotación de funciones. Este tema tiene amplia información disponible en otros trabajos de investigación motivo por el cual no se abarcará en este trabajo.

Planificación de Continuidad de Negocio (BCP) y Recuperación de Desastres (DRP)

Como se ha visto a lo largo del trabajo, los sistemas de TIC son vulnerables a una gran variedad de interrupciones, estas pueden ser leves hasta severas dependiendo de su origen, como desastres naturales o acciones terroristas. Muchas de estas vulnerabilidades pueden ser minimizadas o eliminadas a través de soluciones técnicas, gerenciales u operacionales como parte del esfuerzo de la gerencia de riesgo de la organización, pero es virtualmente imposible eliminar completamente los riesgos.

El BCP se enfoca en sustentar las funciones de negocio de la organización durante y después de alguna interrupción. Un BCP puede ser desarrollado para un proceso específico de negocio o para dar dirección a todos los procesos clave del negocio (Swanson,2002).

El BCP es el proceso de creación de un plan cuyo objetivo asegure que las funciones críticas del negocio pueden soportar una variedad de emergencias (Keele,2005)

En la mayoría de los casos, los recursos críticos residen fuera del control de la organización, con lo que no es posible asegurar su disponibilidad. De este modo, la

planificación, ejecución y pruebas de contingencias efectivas son esenciales para mitigar el riesgo por indisponibilidad de los sistemas y servicios. Según NIST (Swanson,2002), para que un plan de contingencia sea exitoso la gerencia debe asegurarse de:

- Entender los procesos de planes de contingencia de las TIC y su lugar en el macro proceso para los planes de contingencia de operaciones y del negocio.
- Desarrollar o reexaminar las políticas de contingencia y procesos de planificación, y aplicar los elementos del ciclo de planificación, incluyendo preliminares, análisis de impacto en el negocio, selección de sitio alterno y estrategias de recuperación.
- Desarrollar o reexaminar las políticas y planes de contingencia con énfasis en mantenimiento, entrenamiento y ejercicios de los planes de contingencia.

A continuación se definen las etapas para diseñar y elaborar un plan de continuidad de negocio (DRI,2006):

1. Inicio del proyecto.
2. Control y evaluación del riesgo.
3. Análisis de impacto en el negocio.
4. Desarrollo de estrategias de continuidad del negocio.
5. Respuesta a emergencia y operaciones.
6. Desarrollo e implementación de planes de continuidad de negocio.
7. Programas de entrenamiento y concientización.
8. Mantenimiento y ejercicio del plan de continuidad de negocio.
9. Relaciones públicas y coordinación de crisis.
10. Coordinación con autoridades públicas.

1. Inicio del proyecto

1.1 Inicio y control del proyecto

Establecer la necesidad de un plan de continuidad de negocio, que incluya soporte de la gerencia y los elementos para organizar y administrar el proyecto hasta su finalización. Se trabajará con las competencias de:

- Definición de necesidades
- Comunicación de esas necesidades
- Establecer un comité de planificación y dirección.
- Desarrollar los requerimientos iniciales de presupuesto.
- Reporte a la alta gerencia.

1.2 Actividades

El ciclo clásico de planificación de la continuidad del negocio involucra las siguientes etapas:

- Entender asuntos de continuidad de negocio, incremento de concientización y compromiso.
- Planificar el proyecto de continuidad de negocio.
- Análisis y reducción del riesgo.
- Análisis de impacto en el negocio.
- Definición de estrategias de continuidad.
- Desarrollo de planes de continuidad.
- Desarrollo e implementación de procedimientos de planes de continuidad.
- Desarrollo e implementación de entrenamiento y programas de pruebas para el equipo de continuidad.

1.3 Programa o proyecto

Una vez que se inicia el plan, el alcance del proyecto es revisado y las actividades de continuidad son extendidas, el ciclo se repite hasta ser un programa.
La mayoría de las organizaciones ven la continuidad del negocio como un proyecto. Eso esta bien para iniciar el plan, pero la CN debe empapar toda la organización.

1.4 Definición de la necesidad (alcance)

Para las organizaciones entrar en CN por primera vez, asumiendo la gran cantidad de tareas es extenuante. Por eso es crucial obtener adecuadamente el alcance: definir en forma realista los límites para los proyectos y ponerlos en programas generales que eventualmente tomarán ventaja para la protección total de bienes de la empresa.

1.5 ¿Qué es un desastre?

Definir "desastre" es fundamental para la planificación de la CN. Asumir la definición en forma errónea puede causar un desastre, ya sea por invocar un plan no probado y deficiente, o fallando en reconocer potencialmente que existe una condición de desastre hasta que un daño irreparable lo ha causado, los desastres no son siempre evidentes. Debe existir una definición clara de desastre y procedimientos de escalamiento para quejas de clientes, escritorios de ayuda, defectos de calidad, fallas en niveles de servicios e incidentes en producción para que las decisiones puedan tomarse dependiendo del criterio que corresponda con cada desastre.

Según Hiles (2004) para una entidad comercial la definición típica de desastre es: "Un evento, que causa pérdida en un servicio esencial o parte de él, por un periodo de tiempo que pueda poner en peligro al negocio"

Para una organización del sector público, comenta Hiles (2004), la siguiente definición puede aplicar: "Un evento, que causa pérdida en un servicio esencial o parte de él, por un periodo de tiempo que pueda poner en peligro el logro de la misión"

El extracto de la definición necesita ser tangible obteniendo que servicios o instalaciones son esenciales y cuando la duración de esta pérdida podría ser inaceptable. Esto será explorado durante el Análisis de Impacto al negocio.

1.6 Comunicación de la necesidad, concientización

El 80% de los negocios que no tienen plan de continuidad y que experimentan algún desastre, cesan el comercio hasta 2 años. Una compañía puede perder 60% de su productividad en varios días de desastre, haciéndola incompetente(Hiles,2004). Ciertamente los daños de no tener planes de continuidad pueden apuntar a la línea gerencial. Incidentes operacionales reales pueden sobresalir como situaciones que pudieron ser desastres.

La concientización puede incrementar por las amenazas que estén rondando y la pérdida en que se puede ver involucrada la empresa.

Es de mucha ayuda obtener una declaración de patrocinio de la alta gerencia, informando la importancia del proyecto de CN. Es igualmente importante conocer los beneficios del plan:

- Si los riesgos son identificados, el factor de exposición puede ser reducido.
- Mejorar el entendimiento en el negocio (identificando dependencias críticas).
- Mejorar la resistencia operacional.
- Reducir los tiempos fuera de servicio.
- Cumplimiento de regulaciones y requerimientos legales.
- Legislación de compañías que requieran registros mantenidos y protegidos.
- Legislación de registros públicos que requieran mantenimiento y protección.
- Legislaciones de salud y seguridad, que requieran evaluación del riesgo.
- Mejorar la efectividad operacional
- Protección de los bienes.
- Protección de los mercados.
- Mejorar la seguridad y paz mental.
- Evitar acciones legales en contra.
- Demostrar la capacidad de continuidad, dando muestras competitivas y ventajas de mercado.

Es vital para el éxito del proyecto comunicar estos beneficios a la alta gerencia y todos los involucrados con el proyecto de continuidad y los programas subsecuentes.

1.7 Establecer una política de CN

Es de gran ayuda que la alta gerencia defina una política de CN. Esto muestra señales de aprobación para los proyectos de CN y ayuda en su desarrollo, por ejemplo (DRI,2006):

> La organización está comprometida para apoyar efectivamente a los actores miembros del BCP y requiere que se adopten procesos y procedimientos robustos. Esto aplicará para todos los aspectos de la operación de la organización. Todos los procesos serán administrados de acuerdo a procedimientos documentados, que aseguren operaciones consistentes bajo condiciones normales y recuperación rápida en circunstancias anormales.

1.8 Establecer un comité de planificación y dirección

En organizaciones grandes, un comité de dirección necesita ser establecido para:

- Acordar los términos de referencia, alcance y asunciones.
- Acordar Presupuestos y Planes de Proyecto.
- Alcanzar decisiones en prioridades conflictivas.
- Acordar tiempos.
- Entregables.
- Responder a recomendaciones hechas por el equipo de proyecto.
- Hacer disecciones de negocio en asuntos de continuidad.

Este comité necesita representar todos los intereses relevantes y tener la majestad y autoridad para realizar decisiones en asuntos de continuidad (ver Tabla 25).

Tabla 25. Ejemplo de Estructura Comité de Dirección.

Miembros Comité Ejecutivo de Dirección	
Director de Finanzas	Gerentes de Soporte
Director Mercadeo	Gerente de Instalaciones
Gerentes de Unidades de Negocio	Gerente de TIC
Gerentes de Operaciones	Líder de Proyecto de BCP

Fuente: (DRI,2006).

1.9 Planificación del proyecto

Ajustar apropiadamente el proyecto de CN es vital para el éxito y aceptación. Es particularmente importante contar con el alcance y los términos del proyecto para empezar.

Un factor clave para el éxito del proyecto es la selección de un líder, este será el profesional de CN de la organización. Este líder debe ser una persona con habilidades analíticas, juicio sólido y acertado, conocimiento del negocio, competencia técnica, habilidades interpersonales para comunicarse y persuadir a miembros de la gerencia en invertir dinero en algo que nunca va a suceder, conocimiento de gerencia de proyectos y facilidades para trabajo en equipo.

Los roles del proyecto incluyen al líder del proyecto, comité de dirección y donde se desarrollará el proyecto, ya sea clientes internos o externos, representante de ese o gerente de proyecto. Estos roles deben ser claramente definidos y entendidos:

Gerente de proyecto (Líder)

- Trabaja para el cliente en planificar, dirigir, controlar el proyecto en costos y escalas de tiempo.
- Acordar términos de referencia con los clientes.
- Definir los programas y planes del proyecto.
- Revisar y controlar los costos.
- Revisar y controlar el progreso físico.
- Controlar los cambios.
- Trabajar en grupo con todas las partes involucradas.
- Adoptar un estándar de procedimientos de control de proyecto.
- Reportar al cliente el progreso y los costos.
- Asegurar la finalización y entrega del proyecto.
- Usualmente conduce revisiones post-implementación.

Ejecutor

- Interno o externo.
- Responsable de actividades específicas.
- Responsable de la entrega a tiempo y en presupuesto.

Comité de dirección

- Para proyectos largos involucra varios departamentos.
- Aprueba el alcance, planes, presupuestos, términos y referencias.
- Asegura la disponibilidad de recursos.
- Aprueba prioridades, define tolerancia de reportes.
- Firma los entregables y las autorizaciones de las fases siguientes.
- Decide los cambios y monitorea control de calidad/estándares.

Representante del cliente / líder proyecto del cliente

- Responsable por la justificación del proyecto.
- Responsable por el presupuesto del proyecto.

- Reúne con el gerente de proyecto.
- Define términos de referencia.
- Aprueba propuestas.
- Obtiene provisión para presupuesto y autoridad.
- Autoriza el inicio de cada fase.
- Controla todo el rendimiento del proyecto.
- Firma aceptación de proyectos finalizados.

Finalmente, incluir todos los elementos de gerencia de proyectos para la CN.

1.10 Desarrollar requerimientos de presupuesto inicial

1.11 Reportar a la alta gerencia

Los proyectos de CN terminan siendo permanentes una vez que se inician, nunca finalizan. Por eso es tan importante el compromiso de la alta gerencia y el reporte de desviaciones con respecto al progreso general es una herramienta crucial para mantener el ímpetu.

1.2 Control y evaluación del riesgo

La idea es determinar los eventos que pueden afectar en forma adversa la organización, y el daño que pueden causar y el control necesario para prevenir o minimizar los efectos de pérdidas potenciales. Este tema ya se estudio ampliamente con anterioridad, la realización del riesgo se realiza en forma similar al riesgo informático pero varían en tópicos como las vulnerabilidades, amenazas, etc., así que se desarrollará en forma básica y se puede investigar la referencia en caso que el lector necesite profundizar.

1.2.1 Identificación de riesgos potenciales

- Identificar exposición por fuentes naturales, artificiales, tecnológicas, accidentales, internas, etc.
- Determinar la probabilidad de los eventos obtenidos del paso anterior y también:
    - Validar la credibilidad de las fuentes de información.

- Determinar el impacto en la organización.
- Analizar los controles para mitigación.
- Determinar controles adicionales que pueden implementarse.
- Analizar la probabilidad que cada amenaza pueda ocurrir.
- Analizar la probabilidad que un impacto ocurra como resultado de las amenazas identificadas.
- Analizar la efectividad de los controles para mitigación actual y potencial.

- Desarrollar métodos para obtener información.
- Desarrollar métodos para evaluar la probabilidad Vs. severidad.
- Establecer soporte para el proceso de evaluación
  - Preparar análisis costo/beneficio.
  - Preparar presentación ejecutiva que resuma el análisis de los resultados y fuentes de información.
  - Demostrar la validez de la información presentada con los resultados de las pruebas.
- Identificar asuntos legales/reguladores

1.2.2 Determinar la exposición por pérdidas potenciales

- Establecer un proceso para evaluar las pérdidas potenciales identificadas.
- Categorizar la exposición.
- Ranking de las exposiciones (puede ser por factor de ocurrencia o impacto).

1.2.3 Identificación de controles y salvaguardas que previenen o mitigan el efecto de la pérdida potencial

- Controles ambientales.
- Controles Técnicos.
- Controles operacionales
- Controles de reputación
- Efectividad.

1.2.4 Seleccionar y usar una metodología de análisis de riesgo

1.2.5 Identificar e implementar actividades de recolección de información.

- Desarrollar una estrategia consistente con el negocio y la política organizacional.
- Desarrollar una estrategia que pueda ser manejada a través de las divisiones del negocio y sus localidades.
- Desarrollar formas de evaluación del riesgo.
- Crear métodos organizacionales para recolección y distribución de la información.

1.2.6 Evaluar la efectividad de controles y salvaguardas.

- Establecer acuerdos de niveles de servicios de CN para proveedores y clientes (internos y externos) de la organización.
- Desarrollar opciones preventivas y pre-planificación.
- Entender las opciones para gerencia del riesgo y la selección de las respuestas apropiadas en costo/efecto.

1.2.7 Identificar y evaluar los riesgos, controles y su mitigación.

- Establecer diferentes escenarios de desastre basados en riesgos que la organización está expuesta.
    - Severidad en magnitud.
    - Ocurre en el peor tiempo posible.
    - Resulta en impedimento para que la organización continúe con el negocio.

1.2.8 Alternativas

Implica evaluar

- los riesgos.
- el impacto de las exposiciones y riesgos en aquellos factores esenciales para conducir operaciones de negocio

- controles y recomendar cambios, si es necesario, reducir el impacto debido a los riesgos y exposiciones.

1.2.9 Seguridad

- Identificar los posibles factores de exposición de la organización.
- Evaluar los controles existentes de seguridad y sus procedimientos.
- Desarrollar recomendaciones para controles de seguridad improvisados y sus procedimientos.

1.2.10 Gerencia de registros vitales

- Identificar la necesidad de registros vitales, incluyendo electrónico y papel.
- Evaluar procedimientos existentes de respaldo y recuperación de registros vitales.
- Desarrollar recomendaciones para mejorar los procedimientos de respaldo y recuperación.

1.2.11 Documentar y presentar los hallazgos.

1.2.12 Documentar la aceptación del riesgo.

- Determinar y acordar el costo de "fuera de servicio".
- Asegurar que los acuerdos en niveles de servicio están documentados y considerados en términos de interdependencia.
- Desarrollar una matriz con la prioridad de los riesgos que muestre los riesgos técnicos y de negocio.
- Discutir con la alta gerencia y asegurar que ellos acepten el documento de riesgos.

1.2.13Implementar medidas y procedimientos de respaldo, recuperación y seguridad

Análisis de impacto en el negocio.

El Análisis de Impacto en el Negocio es la consecuencia que resulta de una interrupción que puede afectar la organización y las técnicas que pueden ser usadas para cuantificar y calificar ese impacto. Los elementos clave son: establecer el proyecto, escoger el método de recolección de datos (impacto datos) ya sea en cuestionarios, entrevistas o talleres, y por ultimo un reporte.

¿Qué es un BIA?

Por sus siglas en ingles (BIA), el Análisis de impacto en el negocio es la identificación del efecto en la organización que los riesgos puedan tener (Hiles,2004).
Es la identificación de las funciones críticas del negocio en la organización y la determinación del impacto en el negocio al no llevar a cabo esas funciones en un tiempo aceptable (SORM,2006).
Lo ideal es tratar de obtener la mayor información posible sin ser repetitivos ni malgastar el tiempo, se trata de usar el BIA para lograr un número de objetivos al mismo tiempo:

- Identificar los costos financieros o no.
- Establecer la ventana de tiempo en que la recuperación debe realizarse.
- Identificar los materiales vitales y registros necesarios para recuperación y continuidad.
- Hacer una evaluación preliminar de los recursos requeridos para recuperación y continuidad.
- Proveer entrada a la evaluación de riesgos que no se hayan identificado.
- Incrementar la conciencia de CN y empezar a enfocar a los individuos en su responsabilidad potencial, soluciones posibles y costos.

El Proyecto BIA

En organizaciones grandes, el BIA puede ser un proyecto aparte. La logística es considerable ya que es muy probable tener que recolectar información de personas que geográficamente no estén fácilmente disponibles, que estén operando y no se puedan detener en su trabajo, que representen cruce de funciones y conocimiento de procesos y dependencias corporativas. Se deben recolectar datos que resalten las áreas criticas para la misión, cuales son sus valores, de que dependen y por cuanto tiempo pueden sobrevivir sin esas dependencias. Se debe establecer si una instalación se pierde:

- ¿Como impacta la supervivencia de la compañía?
- ¿Como impacta las ganancias de la compañía?
- ¿Como impacta la imagen de la compañía?
- ¿Como impacta a los clientes más importantes, oficinas, productos y servicios?
- ¿Es crítico el tiempo?
- ¿Detiene las funciones críticas de la misión de la organización?
- ¿Puede el cliente prescindir de ellas?
- ¿Qué alternativas hay para lograr los mismos entregables?

La urgencia variará dependiendo de la hora, día o mes.

Métodos de recolección de datos

Existen varias vías de comprometer el BIA, desde cuestionarios de alto nivel hasta muy detallados. Deben incluir:

- Análisis de factores críticos de éxito.
- Revisión de los indicadores clave de rendimiento.
- Flujo de procesos.
- Categorización de actividades.
- Revisión de documentación.
- Entrevistas
- Talleres.

Definición de Factores Críticos de Éxito.

La CN trata de asegurar las actividades críticas para la cumplir la misión y mantenerla durante un desastre. Primero se necesita definir que es un factor crítico de éxito y luego identificar los procesos que los soportan. Tomando esto en cuenta, se pueden revisar las instalaciones y bienes que dependen los procesos que los soportan, esta técnica se llama análisis de factores críticos de éxito, con lo cual Richard Caralli (2004) define factor crítico de éxito como:

- La definición de áreas de rendimiento clave esenciales para que la organización cumpla su misión.
- Número limitado de áreas en que los resultados aseguran el éxito y rendimiento para la organización; son las algunas de las áreas donde todo debe salir bien, si los resultados de esas áreas no son adecuadas, los esfuerzos de la organización serán menores a lo acordado (Hiles,2004).

Los procesos de negocio que soportan la mayoría de los factores críticos de éxito deben recibir mayor prioridad para la recuperación, es necesario seguir explorando para identificar que procesos de negocio dependen cuales bienes.

Indicadores clave de rendimiento

Las metas de negocio de alto nivel es necesario disgregarlas en factores críticos de éxitos efectivos y muy específicos, e indicadores clave de rendimiento que puedan ser monitoreados. La mayoría de las organizaciones han identificado sus indicadores clave de rendimiento. Estos son estadísticas que muestran como es su comportamiento para lograr la misión, metas y objetivos del negocio. Si se pueden identificar los procesos responsables de entregar lo que miden los indicadores clave de rendimiento, se ha identificado los procesos de alto nivel que se necesita proteger y faltaría la asignación de prioridades.

La recolección de la información puede realizarse mediante la revisión de la documentación entregada, cuestionarios, entrevistas y talleres. Es importante hacer una revisión exhaustiva de esta documentación para conocer la organización, sus procesos, la forma más oportuna de obtener la información y continuar con las actividades siguientes.

Justificación

El BIA examina los riesgos y evalúa el impacto de su ocurrencia. La creación de un plan de continuidad de negocio puede estar justificada en algunos de los siguientes argumentos:

- Seguridad y vida.
- Política/Mercadeo (reputación, imagen, clientes, etc.).
- Financiero.
- Cumplimiento con requerimientos legales.
- Calidad.

Cuando sea posible, el impacto debe ser cuantificado en términos financieros y se debe tener cuidado para evitar cuentas dobles.

Matriz de impacto

La vía estándar para continuar con el BIA es la elaboración de una matriz de riesgo y pérdidas potenciales. Como se identifican en párrafos anteriores, las amenazas son pesadas por la probabilidad. Las estadísticas de la industria son la base para la probabilidad de ocurrencias. A continuación se muestran dos métodos para producir la matriz de impacto en el negocio:

1. Resultados por puntaje: Cuando existe una posibilidad significativa de ocurrencia, se puede pesar con rango entre 1-5, donde uno una posibilidad baja y 5 una posibilidad alta de ocurrencia. De manera similar, el impacto financiero también se le puede asignar un peso, dependiendo del tamaño de la empresa, una pérdida de 10.000.000 de US$ puede tener un nivel nocivo o catastrófico, asignando entonces un peso entre 1 y 5. La multiplicación de ambos resultados genera la probabilidad e impacto en las pérdidas. Por ejemplo (ver Tabla 26):

Tabla 26. Ejemplo de Riesgo.

Ejemplo Riesgo	
Riesgo	Fuego
Activo	Planta generadora electricidad
Probabilidad	Muy Alta (4 puntos)
Impacto	Catastrófico
Probabilidad (4) x Impacto (5)	20 resultado total

Fuente: (DRI,2006).

Una tabla simple se puede generar acumulando los resultados más altos en aquellas áreas de riesgo con impacto más serio. Si bien parece simple el método de cálculo, puede resultar en un gran número de probabilidades (empresas grandes) dificultando la asignación de prioridad.

2. Resultados anualizados por costos: a menudo las estadísticas locales están disponibles por planificadores de emergencias o aseguradoras, identificándola probabilidad de ocurrencia. Si la instalación tiene un valor de 45.000.000 US$. Si la probabilidad anualizada se multiplica por el valor total generaría la pérdida estimada, repitiendo el proceso de igual forma por cada bien en riesgo generando un estimado acumulado anualizado.

Ventana de tiempo para recuperación

Un BIA efectivo evalúa el impacto de un desastre en el tiempo. Típicamente, hay un espacio de respiro antes que este se empiece a sentir. La longitud del tiempo depende de los procesos y de la industria. En operaciones financieras de tiempo real, las ventanas de tiempo pueden ser minutos, para otras organizaciones pueden ser días o tal vez semanas. Luego, muchas organizaciones cierran en fines de semanas, algunas en vacaciones colectivas, otras días festivos públicos. El análisis de impacto debe identificar cual es esta ventana de tiempo y porque fase de recuperación debe ser tomada en cuenta. Esta ventana de tiempo es conocida como interrupción máxima aceptable (conocida como MAO por sus siglas en inglés).

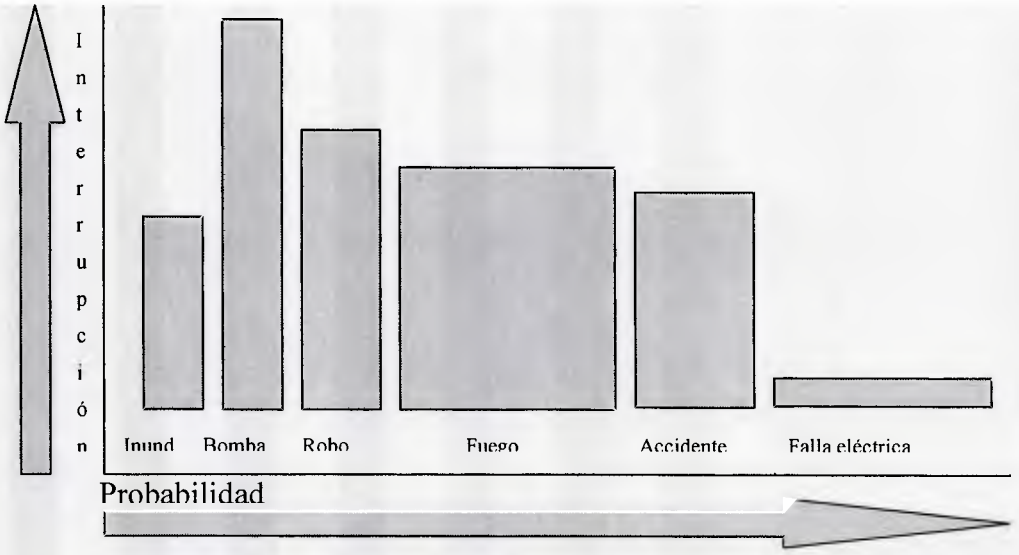

Figura 16. Interrupción y Riesgo.
Fuente: (DRI,2006).

Existen diferentes causas de desastre que pueden ocurrir con mayor frecuencia que otras, y si ocurren implicarían interrupciones en las instalaciones por grandes periodos de tiempo. La Figura 15 identifica las características de los riesgos típicos, donde el alto de cada columna representa ampliamente la longitud de la interrupción y el ancho representa la probabilidad de ocurrencia.

Es necesario entender las pérdidas acumuladas cada minuto, horas y días hasta el punto en que las pérdidas sean insostenibles, eso identificará la ventana de tiempo (ver Figura 17).

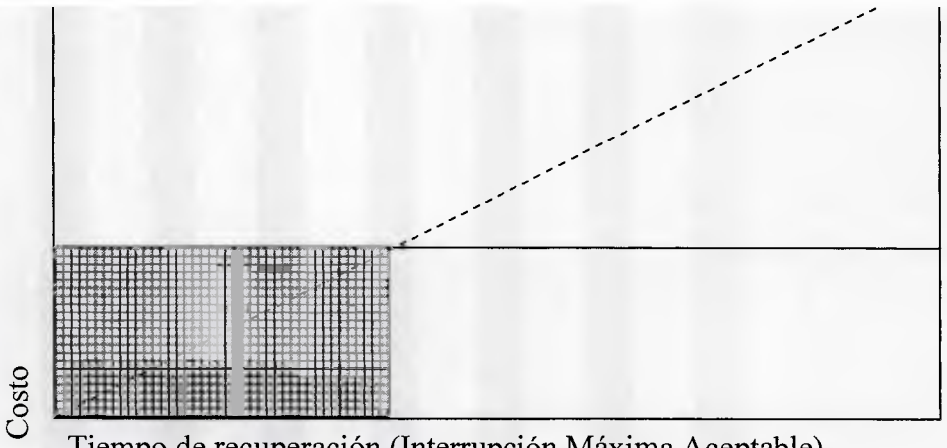

Figura 17. Ventana de tiempo para la recuperación.
Fuente: (DRI,2006).

En la práctica, las pérdidas tal vez no sean una línea recta, ellas tal vez se acumulen gradualmente y repentinamente se vuelvan exponenciales, es importante identificar cuando es el caso.

Recursos

Los requerimientos de recursos para la recuperación a veces son subestimados y se asume que se necesita menos capacidad después de un desastre que en las operaciones normales de producción. En realidad, más capacidad es requerida en términos de equipos operacionales, capacidad de cómputo y telefonía, es importante tener esto presente.

Desarrollo de estrategias de continuidad

El Análisis de Riesgo y el BIA proveerán la justificación para la estrategia de CN y, subsecuentemente el desarrollo del Plan de CN. Con el plan de CN, todavía pueden existir desastres que causen pérdidas en las instalaciones y equipos, sin embargo, la estrategia y el plan deben reducir la probabilidad de desastre y, si ocurre, mitigar el daño y asegurar la retención de la base del cliente y el mercado. La clave para una

estrategia de CN exitosa es focalizarse en los entregables más que en la entrega de procesos. Las preguntas clave son: ¿Cuales son los entregables críticos para la misión de la organización? ¿Cuál es el objetivo de entregarlos (cliente o organización)?
Para una estrategia efectiva de continuidad es necesario un entendimiento claro del negocio y una definición efectiva del alcance del proyecto.

Material Vital

El material vital es cualquier cosa portátil que es necesario para facilitar la recuperación de las operaciones, son cosas como:

- Capacidad de reconstrucción.
- Protección de los bienes de la compañía.
- Protección de los derechos de los accionistas.
- Protección de los derechos de los empleados.
- Cumplimiento del compromiso con los clientes

Los ítems pueden incluir:

- Sistemas de respaldo y software de aplicaciones.
- Datos de transacciones y progreso de trabajo.
- Formas originales y registros para copias.
- Procedimientos operacionales, de aplicaciones y administrativos.
- Contratos de clientes y proveedores.
- Políticas de seguros.
- Detalles de contactos, internos y externos.
- Planos, dibujos, etc.
- Lista de servicios con prioridades y escalas de tiempo.
- Acuerdos con el sitio en Standby.
- Claves de acceso.
- Listas de chequeo.
- Formas de pago.
- Sellos de la compañía.
- Ítems para evaluación del daño y equipo de salvamento.

El método de respaldo y la estrategia de recuperación deben permitir la recuperación dentro del rango máximo aceptable (MAO) y el objetivo de punto de recuperación (RPO).

Opciones

El diseño de planes de CN efectivos empiezan con la identificación del peor escenario post-desastre posible. Si el desastre actual no es tan malo, entonces las partes apropiadas o un subconjunto de lo planes de CN pueden ser usados. La alternativa, diseñar un plan que se ajuste a escenarios específicos no es la mejor, ya que la probabilidad apunta a que el desastre sea diferente al que se está planificando. Mientras más escenarios se desarrollen en el análisis de riesgo, cuando se desarrolle el plan de CN, los resultados hablarán por si solos.

Como todas las inversiones, el plan de CN debe representar el mejor valor por el dinero, seleccionando la mejor estrategia es la clave. Algunas opciones se mencionan a continuación:

- Bunker
- Procesamiento continuo.
    - Equipos de clustering.
    - Arreglos de disco.
    - Espejo de datos.
    - Procesamiento Standby.
- Distribución de procesamiento.
- Sitio Alterno
    - Hot site: ambiente total de producción (hardware, software, datos y comunicaciones) disponible para uso inmediato.
    - Warm site: ambiente en standby, con disponibilidad no inmediata de recuperación.
    - Cold site: ambiente standby sin hardware
- Suministro rápido de necesidades.
- Almacenamiento fuera de sitio.
- Trabajo desde el hogar.

- Acuerdos recíprocos.
- Outsourcing.

Acuerdos contractuales para recuperación de servicios.

En teoría los sitios hot o warm están disponibles 24x7x365. Estos sitios cuentan con un equipo de gente que asiste con la recuperación. Los equipos se mantienen actualizados, mientras otros permanecen soportados. Siempre están disponibles para uso y ofrecen periodos de prueba una o dos veces al año. Pero es importante revisar los acuerdos con la compañía que brinda los servicios del sitio y la recuperación, para no incurrir en fallas por no definir bien los tiempos, ocasionando retrasos y posiblemente incumplimiento.

Respuesta a emergencias y operaciones

Algunos tipos de emergencias se señalan a continuación:

- Terrorismo.
- Daño ambiental (químicos, contaminación, radiación, etc.).
- Desastres (inundaciones, huracanes, tornados, heladas, terremotos, tsunamis, insurrecciones, guerras, etc.).
- Secuestro.
- Ataques armados.
- Violencia en sitio de trabajo.
- Contaminación de productos.
- Reposición de productos defectuosos.
- Descubrimiento inesperado de productos dañinos.
- Pérdida de imagen por actos accidentales o deliberados.
- Fraude.

Coordinación con autoridades públicas

Esta área trata de establecer procedimientos apropiados y políticas para coordinar la continuidad y restauración de actividades con las autoridades locales asegurando el cumplimiento de las leyes locales y regulaciones. Esto puede incluir:

- Coordinación de preparación de procedimientos de emergencias, respuestas, recuperación y restauración con las autoridades locales.
- Establecer procedimientos de preparación para escenarios de emergencias/desastres.
- Mantener conocimiento actual de leyes y regulaciones concernientes a procedimientos de emergencias.
- Las autoridades públicas tal vez puedan ser locales, estatales o nacionales, cada país tiene sus propios procedimientos. El plan de CN debe aceptar que las autoridades locales y públicas pongan límites en la libertad de actuación de las organizaciones después que ocurre un desastre.

Relaciones públicas

Competencias

Desarrollar, coordinar, evaluar y ejercer planes para manejar los medios durante situaciones de crisis.

Desarrollar, coordinar, evaluar y ejercer planes para comunicarse de la manera más apropiada con los empleados y sus familias, clientes clave, soportes críticos, accionistas y propietarios, y gerencia corporativa durante una crisis.

Asegurar que todos los actores estén informados en base a la necesidad.

Comunicación en crisis

La desinformación, incomprensión y conflicto crecen frecuentemente porque una parte comunica las cosas antes de verificar la información, es importante asegurar las fuentes y los sucesos antes de publicar los acontecimientos, es importante no admitir la ambigüedad.

Salvamento y restauración

Después de un desastre, los equipos, las instalaciones, los documentos y los medios de computación pueden lucir irrecuperables, pero el daño puede ser menor a lo que aparenta. Sin embargo, el salvamento debe iniciarse tan pronto como sea posible, por óxido, corrosión y moho pueden hacer la recuperación casi imposible.

Usualmente las organizaciones están aseguradas por pérdidas de bienes tangibles y también por pérdidas en las ganancias y posiblemente en costos extra de trabajo. Sin embargo el asegurado debe tomar algunos pasos para mitigar el costo a los aseguradores, es aquí donde el salvamento juega un rol importante.

Desarrollo e implementación del Plan de Continuidad de Negocio

La información necesaria para el plan de CN ha sido identificada a lo largo de las etapas anteriores, Evaluación del Riesgo, BIA y estrategias.

El plan de desarrollo debe resultar en un plan estructurado, es necesario:

- Decidir la estructura y formato del plan.
- Determinar el provecho de las fases clave del plan.
- Obtener datos y crear el borrador del plan.

El plan resultante debe:

- Introducir:
    - Alcance del plan.
    - Declarar explícitamente las asunciones en que el plan esta basado.
    - Definir "desastre".
    - Mostrar el proceso de escalamiento desde que ocurre el incidente hasta la declaración del desastre.
    - Cubrir procedimientos de alertas, invocaciones y "stand down".
    - Explicar como usar el plan.
- Identificar equipos gerenciales y departamentales y sus roles.
- Identificar los equipos líderes y sus miembros alternos, los miembros del equipo y sus alternos también.
- Identificar y asignar prioridad a las tareas, acciones y funciones a ser emprendidas durante la recuperación.

- Asignar roles y responsabilidades a los líderes y miembros de equipo.
- Identificar localidades alternativas para realizar el trabajo.
- Proveer detalles de contacto para contactos internos y externos.
- Identificar documentos y materiales vitales, incluyendo respaldos, y especificar formas de acceso.
- Identificar requerimientos de recursos, donde se muestre como se brindarán y establecerán escalas de tiempo para su provisión.
- Establecer procesos de reporte y requerimientos.
- Proveer registros de auditoria de las acciones tomadas en la recuperación.
- Mantener estado confidencial, control de versiones y administración de la configuración de documentos para asegurar que todos los planes de CN en circulación son la última versión.

Programas de concientización y entrenamiento

La idea de esta etapa es crear conciencia corporativa y mejorar las habilidades requeridas para desarrollar, implementar, mantener y ejecutar el plan de CN. Para desarrollar el programa satisfactoriamente se deben comprender y ejecutar las actividades que a continuación se muestran.

Establecer los objetivos y componentes del programa

El programa puede estar dividido en dos partes:

- Incrementar la conciencia de aquellos que es imperativo su compromiso para hacer del proyecto de CN un éxito, sin que sean parte del equipo de CN.
- Entrenar a los individuos que tienen un rol dentro de CN.

Estos últimos deben incluir en el programa:

- Identificar los equipos de líderes iniciales y miembros, sin los alternativos.
- Conducir análisis de brechas en sus habilidades para establecer cuales son las habilidades adicionales requeridas.
- Identificar oportunidades de entrenamiento internas y externas.

El entrenamiento debe:

- Identificar requerimientos funcionales de concientización y entrenamiento

- Desarrollar metodologías de entrenamiento
- Adquirir o desarrollar ayuda de entrenamiento
- Identificar oportunidades de entrenamiento externas
- Identificar vehículos para la concientización corporativa.

Ejercicios del BCP

Una vez desarrollado todo el plan de CN es importante ejercitarlo para verificar la cohesión y sinergia de todos los involucrados y el nivel de conciencia en el plan de la organización, a continuación se muestra como se puede desarrollar el ejercicio.

Auditoria y revisión del BCP

Se deben conducir auditorias o revisiones por alguien que no pertenezca al equipo del plan de CN. El plan es actualizado con las recomendaciones que la revisión sugiera antes que sea ejercido. Cada borrador debe ser revisado o auditado por completo antes de realizar las pruebas, el proceso de auditoria debe incluir los siguientes pasos:

- Objetivos y alcance de la auditoria.
- Evaluar y seleccionar el método de la auditoria
- Cubrir los aspectos administrativos,
- Auditar la estructura, contenido y sección de acciones del plan de CN.
- Auditar la documentación de control del plan de CN.

Las áreas a inspeccionar incluyen:

- Introducción.
- Consideraciones corporativas.
- Prioridades funcionales y estrategias de contingencia.
- Invocación del plan y notificación.
- Equipos de CN
- Sitios standby y servicios.
- Procedimientos de respaldos fuera de sitio.
- Recursos de contingencia.
- Entrenamiento y ejercicios.
- Mantenimiento.

Necesidad del ejercicio

La mejor forma de saber que algo funciona es probándolo. Alrededor del 40% de las organizaciones con planes de CN los han probado. Muchos no tienen estrategias coherentes y los resultados de otros incrementan en confidencialidad por su efectividad. El 80% de los planes, cuando se prueba inicialmente muestran sus debilidades, pudiendo ajustarlas y arreglar el plan para hacerlo exitoso, para los casos de la realidad (DRI,2004).

Plan de recuperación de desastres

El plan recuperación de desastres es el proceso de rescatar el acceso a los datos, al hardware y al software necesario para continuar operaciones de negocio críticas después de un desastre. Un plan de recuperación de desastre (DRP) debe también incluir los planes para hacer frente a la pérdida inesperada o repentina de personas clave, aunque el foco es la protección de los datos. DRP es parte de un proceso más grande conocido como plan de continuidad del negocio (BCP) que se ha desarrollado hasta el momento (DRI,2004).

Como se ha desarrollado ampliamente algunos de los pasos del plan de recuperación de desastres en el plan de CN, se menciona a continuación los pasos para un DRP (MSU,2007).

- Obtención de información.
    - Organizar el proyecto.
    - Realizar BIA
    - Realizar evaluación del riesgo.
    - Desarrollar la estrategia de recuperación.
    - Revisar procedimientos de recuperación y respaldos en-sitio, fuera-sitio.
    - Seleccionar instalaciones alternativas.
- Escribir y probar el plan.
- Mantener y auditar el plan.

Incidentes y Leyes

Manejo de Incidentes

El Manejo de Incidentes es un conjunto de acciones o planes para tratar con intrusos, cyber-robos, negación de servicios y otros eventos relacionados con seguridad computacional (Skoudis,2005). El plan de continuidad de negocio y recuperación de desastres que trate con temas de fuego, inundaciones, y otros eventos relacionados debe incluir enlaces con las acciones del manejo de incidentes. El alcance del manejo de incidentes es más que solo intrusos en las redes, cubre crímenes por "insiders", eventos intencionales o no que pueden causar fallas en la disponibilidad y en la propiedad intelectual. La propiedad intelectual incluye temas de marcas, información propietaria, "trade secrets", patentes, copyrights y trademarks.

Un punto clave que no se debe olvidar es la noción de incidente, el cual es un evento (ocurrencia observable) adverso que puede afectar la confidencialidad, integridad o la disponibilidad de la información en la organización. No importa cuando, pero tarde o temprano los incidentes siempre ocurren.

La mejor forma de minimizar un incidente es definir y entender los procedimientos en caso que ocurran.

Los profesionales en manejo de incidentes dividen el proceso en seis fases (Northcutt,2003): preparación, identificación, contención, erradicación, recuperación y seguimiento. Entender cada etapa y que puede salir mal en cada una de ellas, facilitará una repuesta más metódica y evitará duplicación del esfuerzo. También ayuda a tratar con aspectos inesperados de los incidentes.

Preparación

La meta en la fase de preparación es tener al equipo listo para manejar incidentes, entre los elementos necesarios se tiene:

- Usar técnicas proactivas de prevención de incidentes
    - Parchar las vulnerabilidades conocidas de los sistemas.
    - Establecer conciencia en la organización para el manejo de incidentes.
    - Establecer sistemas de detección de intrusos.

- Establecer políticas de notificación.
- Identificar dispositivos críticos.
- Usar políticas robustas en manejo cuentas.

- Desarrollar apoyo gerencial en la capacidad de manejo de incidentes
  - Crear un plan formal de respuesta a incidentes de seguridad
  - Ilustrar gráficamente un incidente
  - Recolectar históricos de soporte
  - Garantizar autoridad al equipo de respuesta a incidentes
- Seleccionar y organizar los miembros del equipo
  - Escoger equipos locales, centralizados o combinados
  - Actualizar los planes de recuperación de desastres para incluir manejo de incidentes computacionales
  - Establecer un plan de visión y compensación para el equipo
  - Realizar listas de chequeos y diagramas de red.
- Desarrollar plan de comunicaciones en emergencias
  - Crear listado telefónico y establecer métodos para informar rápidamente
  - Crear árboles de notificación de incidentes
  - Establecer un punto de contacto inicial, comando de incidentes y centro de comunicaciones
  - Establecer comunicaciones seguras
- Proveer instalaciones con facilidad de reporte
  - Publicar una lista de indicadores de incidentes.
  - Incentivar los reportes de incidentes.
  - Definir parámetros y requerimientos para escalar incidentes.
  - Mantener formas de reporte para incidentes.
- Realizar entrenamiento a los miembros del equipo
  - Realizar conferencias de actualización y entrenamiento en escenarios.
  - Obtener y adaptar herramientas y técnicas de entrenamiento.
  - Mantener en inventario discos de alta capacidad.
  - Ejecutar juegos de guerra.

- Establecer guías para cooperación inter-departamental
    - Manejo local de incidentes menores.
    - Coordinación cercana con "Help Desk".
- Prestar atención particular a las relaciones con los administradores
    - Reconocer lecturas de archivos de logs.
    - Realizar respaldos regulares.
    - Asegurar que el sistema ejecuta software antivirus con definiciones actualizadas.
    - Ejecutar pruebas de penetración.
- Desarrollar interfaces con agencias de aplicación de leyes y otros equipos de respuesta a incidentes.
    - Familiarizarse con las leyes aplicables
    - Conocer los tipos de leyes que puedan interesar
    - Contactar oficiales de aplicación de leyes locales.
    - Unirse o crear equipos CIRT o FIRST

Identificación

La etapa de identificación involucra determinar cuando un incidente ha ocurrido, y en ese caso su naturaleza. La identificación normalmente empieza cuando alguien notifica una anomalía en un sistema o red. Esta fase también incluye informar y solicitar ayuda del personal que pueda apoyar en el entendimiento y solución del problema. Es importante reconocer que no todas las anomalías son incidentes de seguridad.

- Asignar una persona responsable por el incidente.
- Determinar cuando un evento es o no un incidente.
- Mantener la cadena de custodia.
    - Identificar cada pieza de evidencia.
    - Controlar el acceso a la evidencia
- Coordinar con personas que suministren los servicios de red.
- Notificar al personal apropiado

Contención

La meta de la etapa de contención es limitar el alcance y magnitud de un incidente, mitigar la posibilidad que empeore la situación.

- Desarrollar equipos en sitio que examinen la situación.
    - Desarrollar un equipo de trabajo de máximo 3 personas.
    - Asegurar físicamente el área.
    - Usar encuestas que ayuden a asegurar que la información necesaria es registrada.
    - Revisar la información suministrada en la fase de identificación.
    - Mantener el sistema lo menos alterado posible hasta realizar un respaldo.
- Mantener un perfil bajo.
- Evitar código potencialmente comprometido.
- Respaldar los sistemas (incluye mantener el medio de respaldo seguro).
- Determinar el riesgo de continuar las operaciones.
- Mantener informados del progreso a los propietarios de los sistemas.
- Cambiar las claves (password).

Erradicación

La meta de la erradicación es eliminar o mitigar el factor que resulte del compromiso del sistema de seguridad. El compromiso del sistema puede ser traumático para el propietario, pero si el equipo de manejo del incidente falla en erradicar adecuadamente el problema, y si ocurre otro compromiso, la gerencia puede en forma legítima cuestionar la competencia del equipo de manejo de incidentes.

- Determinar la causa y los síntomas del incidente: usar la información recolectada en la etapa de contención, en caso de no estar claro con un ataque específico, tratar de listar posibilidades basadas en la información suministrada.
- Mejorar las defensas.
- Ejecutar análisis periódicos de vulnerabilidades.
- Remover la causa del incidente.

- Localizar el respaldo más reciente.

Recuperación

La tarea primordial de la etapa de recuperación es retornar al sistema e un estado de operatividad total.

- Restaurar el sistema
- Validar el sistema.
- Decidir cuando restaurar las operaciones.
- Monitorear los sistemas.

Seguimiento

La idea principal es aprender del incidente. Buscar de las lecciones aprendidas ayudaran a desempeñar una mejor función en el futuro, los incidentes requieren tiempo y esfuerzo considerable. Es posible que compañeros de equipo que se vieron involucrados en el incidente hayan sido afectados de alguna manera, es importante saber manejar la situación y tratar de olvidar sucesos no relevantes. Las organizaciones que buscan en la base de lecciones aprendidas, manejan el incidente en forma más precisa y rápida.

Desarrollar reporte de seguimiento: rápidamente de forma que no se olviden aspectos relevantes, asignar tareas a el equipo en sitio, incluir formas que agilicen el reporte, invitar a los afectados para la revisión del borrador, realizar reuniones de las lecciones aprendidas, crear un resumen ejecutivo y enviarlo a la gerencia, implementar las acciones aprobadas.

Las organizaciones que realicen manejo de incidentes, una vez solucionados, deben realizar en caso de ser necesaria la investigación forense necesaria dependiendo de la severidad de la incidencia. Si por alguna causa se genera un problema legal, es importante contar con la evidencia intacta y soportada para poder conocer en detalle el ¿Qué?, ¿Cómo?, ¿Cuándo? y ¿Dónde?

Leyes aplicables a la legislación Venezolana

La Seguridad de la Información es un tema que incumbe a todas las personas que realicen operaciones electrónicas, independientemente del medio usado, ya que como se ha mostrado en diferentes puntos del presente trabajo, la información puede ser vulnerada y usada con fines maliciosos. La legislación venezolana ya ha dado algunos pasos para proteger a los usuarios de medios electrónicos, no es la intención de este trabajo profundizar en los temas de leyes, ya que se escapa de su alcance, pero si promover la información y dar las bases para generar confianza en el mundo informático, ..."La Ignorancia de la Ley no excusa de su cumplimiento. (Articulo 2. Código Civil Venezolano). A continuación se enuncian estas leyes y algunos artículos de interés.

Constitución Nacional

Publicada en Gaceta Oficial N° 5.453 (Extraordinaria) de fecha 24 de marzo del 2000

> *Articulo 28*. Toda persona tiene el derecho de acceder a la información y a los datos que sobre sí misma o sobre sus bienes consten en registros oficiales o privados, con las excepciones que establezca la ley, así como de conocer el uso que se haga de los mismos y su finalidad, y de solicitar ante el tribunal competente la actualización, la rectificación o la destrucción de aquellos, si fuesen erróneos o afectasen ilegítimamente sus derechos. Igualmente, podrá acceder a documentos de cualquier naturaleza que contengan información cuyo conocimiento sea de interés para comunidades o grupos de personas. Queda a salvo el secreto de las fuentes de información periodística y de otras profesiones que determine la ley.
>
> *Articulo 60*. Toda persona tiene derecho a la protección de su honor, vida privada, intimidad, propia imagen, confidencialidad y reputación.
>
> La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y ciudadanas y el pleno ejercicio de sus derechos.
>
> *Articulo 110*. El Estado reconocerá el interés público de la ciencia, la tecnología, el conocimiento, la innovación y sus aplicaciones y los servicios de información necesarios por ser instrumentos fundamentales para el desarrollo económico, social y político del país, así como para la seguridad y soberanía nacional. Para el fomento y desarrollo de esas actividades, el Estado destinará recursos suficientes y creará el sistema nacional de ciencia y tecnología de acuerdo con la ley. El sector privado deberá aportar recursos para los mismos. El Estado garantizará el cumplimiento de los principios éticos y legales que deben regir las actividades de investigación científica,

humanística y tecnológica. La ley determinará los modos y medios para dar cumplimiento a esta garantía.

Ley Especial Contra los Delitos Informáticos

Publicada en Gaceta Oficial Nº 37.313 de fecha 30 de octubre del 2001

Articulo 1. Objetivo de la Ley. La presente Ley tiene por objeto la protección integral de los sistemas que utilicen tecnologías de información, así como la prevención y sanción de los delitos cometidos contra tales sistemas o cualesquiera de sus componentes, o de los delitos cometidos mediante el uso de dichas tecnologías, en términos previstos en esta Ley.

Artículos de Interés

De los Delitos Contra los Sistemas que Utilizan Tecnologías de Información

Artículo 6. Acceso indebido. Toda persona que sin la debida autorización o excediendo la que hubiere obtenido, acceda, intercepte, interfiera o use un sistema que utilice tecnologías de información, será penado con prisión de uno a cinco años y multa de diez a cincuenta unidades tributarias.

Articulo 7. Sabotaje o daño a sistemas. Todo aquel que con intención destruya, dañe, modifique o realice cualquier acto que altere el funcionamiento o inutilice un sistema que utilice tecnologías de información o cualesquiera de los componentes que lo conforman, será penado con prisión de cuatro a ocho años y la multa de cuatrocientas a ochocientas unidades tributarias.

Articulo 11. Espionaje informático. Toda persona que indebidamente obtenga, revele o difunda la data o información contenidas en un sistema que utilice tecnologías de información o en cualesquiera de sus componentes, será penada con prisión de tres a seis años y multa de trescientas a seiscientas unidades tributarias.

..."El aumento será de la mitad a dos tercios, si se pusiere en peligro la seguridad del Estado, la confiabilidad de la operación de las instituciones afectadas o resultare algún daño para las personas naturales o jurídicas, como consecuencia de la revelación de las informaciones de carácter reservado.

Artículo 12. Falsificación de documentos. Quien, a través de cualquier medio, cree, modifique o elimine un documento que se encuentre incorporado a un sistema que utilice tecnologías de información; o cree, modifique o elimine datos del mismo; o incorpore a dicho sistema un documento inexistente, será penado con prisión de tres a seis años y multa de trescientas a seiscientas unidades tributarias.

De los Delitos Contra la Privacidad de las Personas y de las Comunicaciones

Articulo 20. Violación de la privacidad de la data o información de carácter personal. Toda persona que intencionalmente se apodere, utilice, modifique o elimine por cualquier medio, sin el consentimiento de su dueño, la data o información personales de otro o sobre las cuales tenga interés legítimo, que estén incorporadas en un computador o sistema que utilice tecnologías de información, será penada con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias.

Articulo 21. Violación de la privacidad de las comunicaciones. Toda persona que mediante el uso de tecnologías de información acceda, capture, intercepte, interfiera, reproduzca, modifique, desvíe o elimine cualquier mensaje de datos o señal de transmisión o comunicación ajena, será sancionada con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias.

De los Delitos Contra el Orden Económico

Articulo 25. Apropiación de propiedad intelectual. Quien sin autorización de su propietario y con el fin de obtener algún provecho económico, reproduzca, modifique, copie, distribuya o divulgue un software u otra obra del intelecto que haya obtenido mediante el acceso a cualquier sistema que utilice tecnologías de información, será sancionado con prisión de uno a cinco años y multa de cien a quinientas unidades tributarias.

Ley de Mensajes de Datos y Firmas Electrónicas

Publicada en Gaceta Oficial N° 37.148 de fecha 28 de febrero del 2001

Objeto y aplicabilidad del Decreto-Ley

Articulo1. El presente Decreto-Ley tiene por objeto otorgar y reconocer eficacia y valor jurídico a la Firma Electrónica, al Mensaje de Datos y a toda información inteligible en formato electrónico, independientemente de su soporte material, atribuible a personas naturales o jurídicas, públicas o privadas, así como regular todo lo relativo a los Proveedores de Servicios de Certificación y los Certificados Electrónicos. ..."La certificación a que se refiere el presente Decreto-Ley no excluye el cumplimiento de las formalidades de registro público o autenticación que, de conformidad con la ley, requieran determinados actos o negocios jurídicos."

De los Mensajes de Datos

Articulo 4. Los Mensajes de Datos tendrán la misma eficacia probatoria que la ley otorga a los documentos escritos, sin perjuicio de lo establecido en la primera parte del artículo 6 de este Decreto-Ley. Su promoción, control, contradicción y evacuación como medio de prueba, se realizará conforme a lo previsto para las pruebas libres en el Código de Procedimiento Civil.

Integridad del Mensaje de Datos

Articulo 7. Cuando la ley requiera que la información sea presentada o conservada en su forma original, ese requisito quedará satisfecho con relación

a un Mensaje de Datos si se ha conservado su integridad y cuando la información contenida en dicho Mensaje de Datos esté disponible. A tales efectos, se considerará que un Mensaje de Datos permanece íntegro, si se mantiene inalterable desde que se generó, salvo algún cambio de forma propio del proceso de comunicación, archivo o presentación.

Constancia por escrito del Mensaje de Datos

Articulo 8. Cuando la ley requiera que la información conste por escrito, ese requisito quedará satisfecho con relación a un Mensaje de Datos, si la información que éste contiene es accesible para su ulterior consulta.

Cuando la ley requiera que ciertos actos o negocios jurídicos consten por escrito y su soporte deba permanecer accesible, conservado o archivado por un período determinado o en forma permanente, estos requisitos quedarán satisfechos mediante la conservación de los Mensajes de Datos, siempre que se cumplan las siguiente condiciones:

1. Que la información que contengan pueda ser consultada posteriormente.
2. Que conserven el formato en que se generó, archivó o recibió o en algún formato que sea demostrable que reproduce con exactitud la información generada o recibida.
3. Que se conserve todo dato que permita determinar el origen y el destino del Mensaje de Datos, la fecha y la hora en que fue enviado o recibido.

Toda persona podrá recurrir a los servicios de un tercero para dar cumplimiento a los requisitos señalados en este artículo.

De la Emisión y Recepción de los Mensajes de Datos

Verificación de la emisión del mensaje de datos.

Articulo 9. Las partes podrán acordar un procedimiento para establecer cuándo el Mensaje de Datos proviene efectivamente del Emisor. A falta de acuerdo entre las partes, se entenderá que un Mensajes de Datos proviene del Emisor, cuando éste ha sido enviado por:

1. El propio Emisor.
2. Persona autorizada para actuar en nombre del Emisor respecto de ese mensaje.
3. Por un Sistema de Información programado por el Emisor, o bajo su autorización, para que opere automáticamente.

Reglas para la determinación de la Recepción

Articulo 11. Salvo acuerdo en contrario entre el Emisor y el Destinatario, el momento de recepción de un Mensaje de Datos se determinará conforme a las siguientes reglas:

1. Si el Destinatario ha designado un sistema de información para la recepción de Mensajes de Datos, la recepción tendrá lugar cuando el Mensaje de Datos ingrese al sistema de información designado.
2. Si el Destinatario no ha designado un sistema de información, la recepción tendrá lugar, salvo prueba en contrario, al ingresar el Mensaje de

Datos en un sistema de información utilizado regularmente por el Destinatario.

Oferta y aceptación de contratos.

Articulo 15. En la formación de los contratos, las partes podrán acordar que la oferta y aceptación se realicen por medio de Mensajes de Datos.

De las Firmas Electrónicas

Validez y eficacia de la Firma Electrónica. Requisitos.

Articulo 16. La Firma Electrónica que permita vincular al Signatario con el Mensaje de Datos y atribuir la autoría de éste, tendrá la misma validez y eficacia probatoria que la ley otorga a la firma autógrafa. A tal efecto, salvo que las partes dispongan otra cosa, la Firma Electrónica deberá llenar los siguientes aspectos:

1. Garantizar que los datos utilizados para su generación puedan producirse sólo una vez, y asegurar, razonablemente, su confidencialidad.
2. Ofrecer seguridad suficiente de que no pueda ser falsificada con la tecnología existente en cada momento.
3. No alterar la integridad del Mensaje de Datos.

A los efectos de este artículo, la Firma Electrónica podrá formar parte integrante del Mensaje de Datos, o estar inequívocamente asociada a éste; enviarse o no en un mismo acto.

La Certificación

Articulo 18. La Firma Electrónica, debidamente certificada por un Proveedor de Servicios de Certificación conforme a lo establecido en este Decreto-Ley, se considerará que cumple con los requisitos señalados en el artículo 16.

Objeto de la Superintendencia

Articulo 21. La Superintendencia de Servicios de Certificación Electrónica tiene por objeto acreditar, supervisar y controlar, en los términos previstos en este Decreto-Ley y sus reglamentos, a los Proveedores de Servicios de Certificación públicos o privados.

Certificados Electrónicos

Garantía de la autoría de la Firma Electrónica

Articulo 38. El Certificado Electrónico garantiza la autoría de la Firma Electrónica que certifica así como la integridad del Mensaje de Datos. El Certificado Electrónico no confiere la autenticidad o fe pública que conforme a la ley otorguen los funcionarios públicos a los actos, documentos y certificaciones que con tal carácter suscriban.

Ley Orgánica de Identificación

Publicada en Gaceta Oficial Nº 38.458 de fecha 14 de Junio del 2006

> Articulo 1. Objeto. La presente Ley tiene por objeto regular y garantizar la identificación de todos los venezolanos y venezolanas que se encuentren dentro y fuera del territorio nacional, de conformidad con lo establecido en la Constitución de la República Bolivariana de Venezuela.
> Articulo 4. Implantación de la Tecnología. El Estado garantizará la incorporación de tecnologías que permitan desarrollar un sistema de identificación seguro, eficiente y coordinado con los órganos del Poder Público.
> El Ejecutivo Nacional por órgano del ministerio con competencia en materia de identificación de los habitantes de la República, vigilará el mantenimiento y la actualización permanente y progresiva del sistema de identificación, con el objeto de lograr un sistema de avanzada tecnología, que facilite a la ciudadanía el acceso a los servicios públicos, el intercambio de información y el apoyo a las funciones de los órganos del Estado.
> Articulo 8. Elementos de Identificación. Son elementos básicos de la identificación de los ciudadanos y ciudadanas: sus nombres, apellidos, sexo, fecha de nacimiento, lugar de nacimiento, los dibujos de sus crestas dactilares y cualquier otro medio de identificación.

Ley para la Protección de Niños, Niñas y Adolescentes en Salas de Uso de Internet, Videojuegos y otros Multimedias

Publicada en Gaceta Oficial Nº 38.529 de fecha 25 de Septiembre del 2006

> Articulo 1. Esta Ley tiene por objeto:
> 2.- Promover el uso adecuado de los servicios de Internet con fines educativos, recreativos y para la libre comunicación entre las personas.
> Articulo 10. Mecanismos de Seguridad. Todas las salas de juegos computarizados, electrónicos o multimedias y de servicios de Internet están obligadas a implementar controles, mecanismos de seguridad y programas en las computadoras y equipos destinados a niños, niñas y adolescentes para hacer cumplir el articulado establecido en esta Ley. Los proveedores de servicios de Internet deberán ofrecer y suministrar a todos sus usuarios y usuarias, de manera gratuita, estos controles, programas y mecanismos de seguridad.
> La Comisión Nacional de Telecomunicaciones, a través de su unidad técnica competente, establecerá mediante normas técnicas los requisitos y condiciones mínimas que deben cumplir los referidos controles, programas y mecanismos de seguridad.
> Articulo 17. Infracción de los proveedores de servicio de Internet. Los proveedores de servicios de Internet que incumplan con la obligación de ofrecer y suministrar a todos sus usuarios y usuarias, de manera gratuita, los

controles, programas y mecanismos de seguridad, de conformidad con lo establecido en el artículo 10 de esta Ley, serán sancionados con multa desde uno por ciento (1%) hasta dos por ciento (2%) de los ingresos brutos causados en el ejercicio fiscal inmediatamente anterior a aquel en el cual se cometió la infracción.

Los órganos rectores en materia de tecnología de información será competentes para imponer esta sanción pecuniaria, mediante el procedimiento previsto en la Ley Orgánica de Telecomunicaciones.

Decreto con Fuerza de Ley de Reforma de la Ley General de Bancos y otras Instituciones Financieras

Publicada en Gaceta Oficial N° 5.555 (Extraordinaria) de fecha 13 de Noviembre del 2001

Atribuciones de la Superintendencia

Artículo 235. Corresponde a la Superintendencia de Bancos y Otras Instituciones Financieras:

10. El establecimiento de las reglas conforme a las cuales deberán practicarse las auditorias prescritas por la ley o las ordenadas por la propia Superintendencia de Bancos y Otras Instituciones Financieras, si fuere el caso; así como, directrices sobre el uso de tecnologías, para una mejor integración de las operaciones bancarias.

Fraude Electrónico

Artículo 445. Quien a través de la manipulación informática o mecanismo similar, con ánimo de lucro, efectúe una transferencia o encomienda electrónica de bienes no consentida, en perjuicio del banco, entidad de ahorro y préstamo, institución financiera o casa de cambio, o de un cliente o usuario, será penado con prisión de ocho (8) a diez (10) años.

Con la misma pena serán castigados los miembros de la junta administradora, directores, administradores o empleados del banco, entidad de ahorro y préstamo, institución financiera o casa de cambio, que colaboren en la comisión de las transferencias antes mencionadas.

Apropiación de Información de los Clientes

Artículo 446. Quien a través de la manipulación informática o mecanismo similar, se apodere o altere documentos, cartas, mensajes de correo electrónico o cualquier otro documento o efecto personal remitido por un banco, institución financiera o casa de cambio, a un cliente o usuario de dicho ente, será penado con prisión de ocho (8) a diez (10) años.

Apropiación de Información por Medios Electrónicos

Artículo 447. Quien utilice los medios informáticos o mecanismo similar, para apoderarse, manipular o alterar papeles, cartas, mensajes de correo electrónico o cualquier otro documento que repose en los archivos electrónicos de un banco, entidad de ahorro y préstamo, institución financiera o casa de cambio, perjudicando el funcionamiento de las empresas regidas por este Decreto Ley o a sus clientes, será penado con prisión de ocho (8) a diez (10) años.

BASILEA II

Establecido en 1930, el Banco de Acuerdos Internacionales (Bank of International Settlements) a través del Comité de Supervisión Bancaria, estableció los estándares prudenciales internacionales para la gestión de instituciones bancarias. Los estándares fueron interpretados a través de las legislaciones y regulaciones correspondientes por cada país. Las nuevas regulaciones capitales de Basilea II (el marco de trabajo revisado) representan uno de los cambios más significativos en el sector financiero de las últimas décadas. Las discusiones empezaron en 1998 con el primer papel de consulta que dio origen al primer marco de trabajo que el Comité de Basilea concluyó en 1994. Las nuevas regulaciones representan un significativo paso adelante en la supervisión bancaria y causará cambios mayores en la organización de los bancos operados internacionalmente (ITGI,2007)

El objetivo de Basilea II es promover la adopción de prácticas de gestión de riesgo para riesgo crediticio y operacional, y fortalecer los enlaces entre el riesgo financiero y sus requerimientos capitales.

Según el comité, el acuerdo trata de:

- Fortalecer la validez y estabilidad del sistema bancario internacional y mantener un estado presente de capitalización en el sistema bancario.
- Mejorar las condiciones en los niveles del campo de juego.
- Brindar dirección a todos los riesgos en forma diligente.
- Asegurar que el capital del banco se adecua para cumplir con los niveles de riesgo y otras transacciones.
- Aplicar de igual forma para los bancos con variación en la complejidad y apetito de riesgo.

El Comité de Supervisión Bancaria de Basilea (2004) escribe en su documento que Basilea II tiene por objetivo construir una base sólida para la regulación prudente del

capital, la supervisión y la disciplina de mercado, así como perfeccionar la gestión del riesgo y la estabilidad financiera.

Requerimientos de Capital Mínimo

Mantenimiento del capital regulatorio calculado por los tres mayores componentes de riesgo que un banco puede enfrentar: crédito, operacional y mercado.
El requerimiento de capital mínimo es determinado por el radio de capital mínimo de 8% basado en el riesgo-peso del bien.

Proceso de Revisión Supervisora

El segundo pilar se concentra en el aspecto cualitativo de las actividades supervisoras. Los supervisores son responsables de asegurar la calidad de los sistemas de gestión de riesgo. Los principios de Basilea II relacionados con TI se pueden ver en la Tabla 27.

Tabla 27. Principios de Basilea II y los aspectos de IT.

Principio Basilea II	Aspecto de TI
Junta Directiva Concienciación de riego operacional Establecer un marco de gestión para el riesgo operacional Aprobación Revisión periódica	Alineación estratégica entre el negocio y TI Valor agregado de TI Gestión del riesgo de TI Medida de rendimiento de TI
Junta Directiva Asegurar auditorias internas y externas efectiva Personal de auditoria interna bien entrenado y competente operacionalmente independiente	Incrementar foco en programas auditorias internas Necesidad de asegurar gobierno de TI fuerte y demostrable Necesidad de un marco de control
Alta Gerencia Implementación consistente de un marco de gestión del riesgo operacional Desarrollar políticas, procesos y procedimientos	Metodologías para enlazar los huecos "Gaps" entre los riesgos de TI, necesidades de control y asuntos técnicos Normas verificables y representativas
Identificación y evaluación Todos los productos materiales, actividades, procesos y sistemas Cambios planificados sujetos precedidos de procedimientos de evaluación	El negocio bancario es altamente dependiente de los sistemas de TI Penetrar en todos los productos, actividades y procesos TI es uno de los mayores factores de riesgo operacional
Monitoreo y reporte Monitorear los perfiles del riesgo operacional Reportes a la junta directiva y alta gerencia	TI es fundamental en cualquier sistema de monitoreo y reporte
Política de control Políticas, procesos y procedimientos de control o mitigación de riesgo operacional	Debido a que TI es esencial para la supervivencia del negocio, debe ser parte significativa en las políticas de riesgo y control del banco
Plan de contingencia Planes de contingencia y continuidad de negocio Minimizar las perdidas durante la interrupción del negocio	Debido a que TI es esencia para la supervivencia del negocio, es prioritario diseñar un plan de recuperación de desastres (DRP)
Supervisión Bancaria Requerimientos para un marco referencial de identificación, acceso y control de riesgos. Evaluación del desarrollo	Debido a que TI es esencial para la supervivencia del negocio, es importante la evaluación periódica del marco referencial

Fuente: (Guldentops,2004).

Disciplina de Mercado

Los bancos deben tener una publicación formal de políticas aprobadas por la junta directiva. Este pilar es diseñado para permitir al mercado tener una mejor visión de la posición de riesgo del banco y así medir las contrapartes para los precios del banco y negociar apropiadamente.

Normativa de Tecnología de la Información, Servicios Financieros Desmaterializados, Banca Electrónica, Virtual y en Línea para los Entes Sometidos al Control, Regulación y Supervisión de la Superintendencia de Bancos y Otras Instituciones Financieras

Publicado por SUDEBAN con vigencia desde 20 julio 2007

Objetivo

La presenta norma tiene como objetivo establecer los lineamientos básicos que deberán cumplir los sujetos sometidos a la supervisión, control y regulación de la Superintendencia de Bancos y Otras Instituciones Financieras en la implantación y uso de la Tecnología de la Información, así como, en la prestación de servicios financieros desmaterializados, banca en línea, electrónica y virtual.

Titulo I - Disposiciones Generales

Capítulo I – Objeto y Ámbito de la Aplicación

Articulo 1: La presente norma tiene como objeto regular la implantación y uso de la Tecnología de la Información de los sujetos sometidos a la supervisión, control y regulación de la SUDEBAN, así como, de la prestación de servicios financieros desmaterializados, banca en línea, electrónica y virtual, con el fin de coadyuvar a minimizar las brechas entre los riesgos de negocio, las necesidades de control y aspectos técnicos orientados a asegurar los servicios de atención al cliente interno y externo; obligándolos a cumplir con los requerimientos de confiabilidad, efectividad, eficiencia, confidencialidad, integridad, disponibilidad y cumplimiento de la información.

Articulo 2: "Las disposiciones de la presente normativa se aplicarán a los sujetos sometidos a la supervisión, control y regulación de la SUDEBAN, en lo adelante Entes supervisados, a saber: Bancos Universales, Bancos de Desarrollo, Bancos Comerciales, Bancos de Inversión, Bancos Hipotecarios, Arrendadoras Financieras, Fondos del Mercado Monetario, Casas de Cambio, Entidades de Ahorro y Préstamo y Bancos Estatales, Empresas Emisoras y Operadoras de Tarjetas de Crédito,..."

Titulo V – Seguridad de la Información

Capítulo I – Políticas de Seguridad de los Activos Informáticos

Artículo 38: El Ente supervisado debe administrar adecuadamente la seguridad lógica de los recursos de Tecnología de Información, incluso aquellos que sean administrados o custodiados por terceros. En consecuencia deberán establecer, formalizar e informar las políticas y procedimientos que permitan identificar, autenticar y autorizar el acceso a los sistemas de información, operativos y de base de datos.

De igual forma, deberán incluir entre sus políticas y procedimientos aquellos que permitan hacer un seguimiento a las transacciones operaciones que sean ejecutadas sobre los activos informáticos.

Artículo 39: En la estructura organizacional del Ente supervisado, debe existir un área de seguridad de la información independiente de las unidades de Tecnología de la Información, Auditoría de Sistemas y Riesgo, estableciéndose como mínimo las siguientes funciones:

a. Definir y mantener actualizadas las políticas de seguridad de la información.

b. Aplicar y asegurar el cumplimiento de las políticas de seguridad de la información definidas.

c. Administrar el acceso a los sistemas operativos, base de datos, aplicaciones, cortafuego, enrutadores, proxys, equipos computacionales y de telecomunicaciones empleados por el Ente supervisado, incluyendo aquellos administrados y custodiados por terceros.

d. Monitorear los procesos de control de cambios y pases a producción de los sistemas y aplicaciones productivas.

e. Realizar el control y seguimiento continuo a los accesos efectuados a los activos de información.

f. Establecer políticas, normas y procedimientos que regulen, controlen y aseguren el seguimiento continuo de la utilización del correo electrónico e Internet y todas aquellas transacciones que son ejecutadas a través de los diferentes canales electrónicos empleados por los clientes.

Capítulo II: Confidencialidad y seguridad de la información.

Artículo 40: Los empleados del Ente supervisado deben firmar un acuerdo de confidencialidad y la no divulgación de información, como parte de sus términos y condiciones iniciales de empleo.

Parágrafo único: El personal temporal o contratado, así como los usuarios externos deben firmar el acuerdo de confidencialidad y la no divulgación de la información, antes que se les otorgue el acceso a las instalaciones de procesamiento de la información. Por otra parte, no deberán tener acceso a las bases de datos del Ente supervisado, en procura de mantener la confidencialidad de la información del cliente.

Artículo 41: El Ente supervisado deberá establecer un esquema de referencia de clasificación o categorización relativa a la confidencialidad de los datos según su nivel de sensibilidad (información confidencial, pública, privada, entre otros).

Artículo 42: Los accesos a los sistemas, aplicaciones o bases de datos deben administrarse a través del uso de perfiles definidos y documentados, los cuales estarán asociados a los cargos, roles o actividades desempeñadas por los usuarios.

Las normas y procedimientos establecidos para la asignación de los accesos deben estar debidamente documentados y formalizados.

Artículo 43: La unidad de seguridad de los activos de información deberá garantizar que los operadores de turno no tengan acceso al ambiente de producción definido en los computadores y servidores de misión crítica del Ente supervisado.

Artículo 44: El Ente supervisado debe establecer políticas y procedimientos para regular, controlar y monitorear la utilización y acceso al correo electrónico e Internet, así como, a los enrutadores, cortafuego y Proxy. De igual forma, deberá generar reportes de auditoria sobre intentos de violaciones a las redes o equipos, detección de posibles delitos informáticos que atentan contra la confidencialidad de los clientes, uso de utilitarios sensitivos y las actividades de los usuarios con atributos de administración y accesos especiales.

Artículo 45: Definir mecanismos que permitan restringir al personal no autorizado el tráfico de datos entrantes y salientes a los recursos tecnológicos de la red. De igual forma, será necesario efectuar pruebas de penetración, tanto internas como externas, en periodos no mayores a un (1) año.

Artículo 46: Establecer dentro de su plataforma de red, aplicaciones que faculten la prevención, detección y eliminación de virus informáticos. El Ente supervisado, deberá asegurarse de la oportuna actualización de la base de datos de virus.

Artículo 47: Restringir el acceso a utilitarios sensitivos que permitan modificar datos en el ambiente de producción, para lo cual deberán documentar, sustanciar y justificar cuando ocurra el evento.

Artículo 48: La plataforma tecnológica del Ente supervisado, debe ser auditada por medio de evaluaciones internas y externas en periodos no mayores a un (1) año. Para ello, el área de auditoría de sistemas deberá definir un plan de trabajo anual que sustente las actividades que serán efectuadas para asegurar el adecuado control interno asociado al uso de la Tecnología de la Información

Capítulo III – Generación de Registros de Auditorias

Artículo 49: Se deben mantener activos los registros o pistas de auditorias generadas por las aplicaciones y sistemas de misión crítica, particularmente en aquellos casos en los cuales exista modificación o alteración de la información almacenada en las bases de datos productivas. De igual forma, deberán asegurar el almacenamiento de los mencionados registros por un periodo de un (1) año.

Por otra parte, las pistas de auditoria deberán ser revisadas por el área de seguridad de la información y auditoría de sistemas, para lo cual será necesario generar informes que reflejen posibles brechas o vulnerabilidades

identificadas. Estos informes deberán generarse anualmente y deben ser entregados a esta Superintendencia, cuando así sea requerido.

Capítulo IV – Seguridad Física

Artículo 50: El Ente supervisado debe contar con una cobertura o una provisión de seguros para los principales equipos de cómputo y telecomunicaciones que permita mitigar los posibles riesgos existentes (incendios, huelgas, motín, impactos de rayo, explosión, implosión, humo, gases o líquidos corrosivos, corto circuito, variaciones de voltaje, robo, asalto y fenómenos naturales).

Artículo 51: Los materiales de construcción del edificio en el cual se almacena el centro de datos, incluyendo paredes, techos y pisos deben ser de materiales no combustibles.

Artículo 52: Las paredes del centro de procesamiento de datos deben extenderse desde la estructura del piso a la del techo del edificio y no desde pisos elevados o techos falsos, con el fin de impedir una entrada subrepticia a las áreas sensibles de la citada instalación.

Artículo 53: Instalar como mínimo un sistema de supresión de fuego de contacto seco en el cuarto que se encuentra el computador central y específicamente dentro de la cinta o discoteca.

Artículo 54: Garantizar el mantenimiento adecuado de los detectores y sistemas de alarma contra incendio, así como de las salidas de emergencia, paneles de distribución eléctrica y de potencia, aire acondicionado, suministros de potencia ininterrumpible (UPS), plantas eléctricas, entre otros aspectos.

Artículo 55: Se debe contar con un sistema de seguridad eléctrica que proteja de las variaciones de voltaje al computador central, sus periféricos y a los equipos de comunicación de datos. Por otra parte, el cuarto de comunicaciones debe tener instalado supresores de corrientes, protectores de las líneas de datos, barras de tierras, entre otros aspectos. De igual forma, debe estar libre de contactos e instalaciones eléctricas en mal estado.

Artículo 56: Se debe ubicar el panel de distribución del sistema eléctrico en un área segura e inaccesible a personas no autorizadas.

Artículo 57: Garantizar la redundancia de los equipos de aire acondicionado instalados en el centro de procesamiento de datos.

Artículo 58: Los centros de procesamiento de datos y telecomunicaciones tanto principales como alternos, deben contar con mecanismos adecuados para la detección y extinción de incendios que aseguren la integridad del personal que reside dentro o cerca de estas instalaciones, así como, la de los activos de información. De igual forma, las mencionadas áreas deben contar con dispositivos de control de la humedad y del clima, mantenerse libres de material inflamable. En este sentido, se deberán realizar simulacros sobre los posibles eventos de contingencia que podrían presentarse en estas instalaciones.

Parágrafo único: El Ente supervisado debe asegurar la existencia de procedimientos que regulen las condiciones ambientales de las instalaciones de procesamiento de datos y telecomunicaciones, tanto principales como

alternos, a fin de asegurar que estos proporcionen un ambiente físico conveniente para su funcionamiento y protejan los activos de información y al personal adscrito al área de Tecnología de la Información contra peligros naturales o fallas humanas.

Artículo 59: Los centros de procesamiento de datos y telecomunicaciones, deben mantenerse separados y claramente definidos por perímetros físicos. De igual forma, deben mantenerse continuamente monitoreados cubriendo para ello, todo el perímetro de sus instalaciones.

Artículo 60: El cableado de comunicaciones debe estar debidamente protegido por canaletas, así como identificado o etiquetado. Por otra parte debe estar separado de los cables de electricidad.

Artículo 61: Los centros de procesamiento de datos y telecomunicaciones, tanto principales como alternos, deben estar resguardados por adecuados controles de acceso, para lo cual se deben considerar los siguientes aspectos:

a. Utilizar controles de autenticación para el acceso del personal autorizado (tarjeta, número de identificación personal –PIN-, carnet, biometría, entre otros).

b. Restringir el acceso a personal no autorizado a las mencionadas instalaciones. Por otra parte, las actividades ejecutadas por los visitantes deben ser supervisadas o inspeccionadas, así como encontrarse registradas en las bitácoras destinadas para tal fin.

c. Revisar y actualizar periódicamente los derechos de acceso a las aras protegidas o restringidas.

Artículo 62: Las instalaciones internas o externas en las cuales se guardan, almacenan y custodian los respaldos de información, deben mantenerse niveles de seguridad similares a los definidos para los centros de datos.

Artículo 63: Los listados y documentación de datos, programas y sistemas deben estar resguardados con adecuadas medidas de seguridad. Se debe definir un procedimiento para determinar la destrucción o desecho de los reportes generados, una vez cumplido su periodo de retención, vigencia o uso.

Titulo VI - Plan de Contingencia Tecnológica

Capítulo I - Alcance y Contenido del Plan de Contingencia

Artículo 64: La Alta Gerencia del Ente supervisado debe asegurar la existencia de un plan de contingencias tecnológicas aprobado, formalizado, actualizado, implementado y probado. El plan debe cubrir como mínimo los siguientes aspectos:

a. Objetivo y alcance del plan definido.

b. Metodología empleada para su diseño.

c. Identificación de procesos críticos.

d. Clasificación de los sistemas, aplicaciones, software y equipos (críticos, vitales, sensitivos, etc.).

e. Prioridad y estrategia de recuperación que involucre cada plataforma de Tecnología de Información en la cual se almacenan y procesan las aplicaciones o datos que soporten una función crítica del negocio.

f. Detalle de cada uno de los procedimientos definidos para la recuperación de operaciones críticas. Sobre este aspecto deberá considerarse el manejo de distintos escenarios para cada tipo de incidencia que puede afectar el funcionamiento y operatividad del Ente supervisado.
g. Localización de los medios de respaldos, así como, del personal autorizado para accederlos.
h. Identificación del personal de contacto por área y descripción de sus responsabilidades.
i. Niveles de escalamiento para el manejo y resolución de las fallas existentes o detectadas.
j. Recursos humanos, financieros y tecnológicos mínimos y necesarios para la recuperación de la operatividad del negocio.
k. Documentación asociada a los contratos o convenios realizados con terceros o proveedores externos de tecnología de información para apoyar el proceso de recuperación.
l. Establecimiento del periodo de recuperación crítico para los recursos de información, en el cual debe restablecerse el procesamiento del negocio, antes de que se experimenten pérdidas significativas o inaceptables.

CAPITULO III
MARCO METODOLÓGICO

Tipo y Diseño de la Investigación

Una vez realizada la revisión de la literatura y la teoría que apoya el presente trabajo se profundiza en la investigación, señalando el tipo y diseño a realizar y a partir de éstos las estrategias y acciones que se adecuan a las características y objetivos de la investigación.

Aunque existen diferentes tipos de clasificación para las investigaciones, estas se pueden dar partiendo del origen de la información en Documental y de Campo (Peñaloza,2005). El diseño de investigación Documental es referido a la indagación de problemas a nivel teórico y en la cual la información requerida para abordarlos se encuentra básicamente en materiales impresos, registros, estadísticas, reportes, etc. Las investigaciones de Campo se caracterizan porque los problemas que estudian surgen de la realidad y la información requerida debe obtenerse directamente de ella.

Si bien se ha encontrado documentación completa en el área de Seguridad de la Información, las investigaciones realizadas en Venezuela en esa área son pocas con respecto a los fundamentos teóricos planteados en este trabajo. Tampoco en las investigaciones encontradas se han hallado evidencias de trabajos de campo que hayan recolectado información, por este motivo este trabajo de investigación sigue un tipo de investigación Documental y de Campo.

Los tipos de investigación de campo se pueden dividir de acuerdo al nivel de profundidad con que se abordan en: exploratoria, descriptiva, explicativa, y evaluativo, se mencionan estas porque son las más comunes encontradas en los distintos autores de bibliografía en metodología de la investigación.

El carácter del tipo de investigación desarrollado es evaluativo, por cuanto el objetivo principal del trabajo es evaluar la aplicación del Desarrollo de los Fundamentos Teóricos de Seguridad de la Información en la Banca Comercial y Universal de Venezuela. Uno de los objetivos del presente Trabajo de Grado de Maestría es recoger información conjunta sobre las variables definidas (ver Tabla 28) y así mostrar ciertos criterios y controles como lo definen las mejores prácticas.

El diseño de la investigación usada el presente Trabajo de Grado de Maestría será no experimental ya que no se realiza manipulación alguna de las variables definidas.
Aunque recolectar la información que se necesita en el desarrollo del trabajo puede tardar un tiempo largo, los cambios en el área de seguridad de la información se dan de manera menos rápida en comparación con el tiempo estimado de recolección. Además, no interesan los datos para hacer inferencias respecto al tiempo y el cambio de los determinantes, sino explorar y describir las variables para dar su estado del arte, es como tomar una foto de los bancos pertenecientes a la Banca Comercial y Universal en un periodo de tiempo dado, motivo por el cual el diseño es no experimental transeccional.

Población y Muestra

La población según Mendenhall (1981) es el conjunto de todas las mediciones de interés para el investigador que concuerdan con determinadas especificaciones, en el caso del trabajo en cuestión, como lo indica el titulo, se limita a las organizaciones del Sector Bancario de Venezuela, de la Banca Comercial y Universal, estas son 37 instituciones (Asobanca,2007).
La muestra es entendida como un subconjunto seleccionado de la población de interés para el estudio. En un esfuerzo por tomar una muestra representativa, se realizó la selección de individuos característicos subjetivamente que constituyen una modalidad de muestreo no probabilístico por conveniencia, donde el juicio y la intuición del investigador constituyen un reflejo adecuado de la población. Para la presente investigación se procedió a seleccionar el personal perteneciente a la Banca Comercial y Universal que cumpliera con los siguientes requisitos:

- Personal profesional especializado en su organización en el área de Seguridad de la Información.
- Personal perteneciente a la Gerencia de Seguridad de la Información o su equivalente.
- Compromiso de confidencialidad entre el investigador (o personal allegado en la empresa donde labora) y la institución financiera perteneciente a la Banca

Comercial y Universal, ya que el tema a tratar tiene mucha sensibilidad, dada la naturaleza del negocio.

- Mantener los acuerdos de confidencialidad del personal y la organización a la que pertenecen en el suministro de información.

Posterior a la verificación de los requerimientos descritos anteriormente, se entregó el instrumento a todos los posibles miembros de la población que cumplían los criterios de selección, para su respectiva aceptación, rechazo o descarte.

Definición de las Variables

Para la presente investigación las variables estudiadas se muestran a continuación:

Tabla 28. Variables de la Investigación

Definición nominal	Rel. Obj.	Objetivo Variable	Definición operacional
Gestión Riesgo Informático	2, 4, 5	Identificar, cuantificar y asignar prioridad a los riesgos según el criterio de aceptación y objetivos relevantes para la organización	• Gestión Riesgo Informático
Políticas, estándares y procedimientos	2, 4, 5	Brindar dirección gerencial y soporte a seguridad de la información de acuerdo con los requerimientos del negocio, leyes y regulaciones relevantes	• Políticas, estándares y procedimientos
Clasificación de la información	2, 4, 5	Asegurar que la información recibe el nivel apropiado de protección	• Clasificación de la Información
Seguridad física y ambiental	2, 4, 5	Prevenir el acceso no autorizado, daño, o interferencia a las instalaciones e información	• Seguridad Física y Ambiental
Seguridad en RRHH	2, 4, 5	Asegurar que los empleados, contratistas y terceros entiendan sus responsabilidades, y que se ajustan para los roles que han sido considerados, y reducir el riesgo de robo, fraude, o uso de las instalaciones	• Seguridad en RRHH
Gestión de comunica. y operaciones	2, 4, 5	Asegurar la correcta y segura operación de las instalaciones y procesamiento de la información	• Control de Cambios • Segregación de funciones • Separación desarrollo y producción • Gestión servicios 3ros • Planificación y aceptación sistemas • Protección contra código malicioso • Respaldos • Gestión Seguridad en Redes • Manipulación de Medios • Intercambio de Información • Servicios de Comercio Electrónico • Monitoreo y Control
Control de acceso	2, 4, 5	Controlar el acceso a la información	• Gestión de acceso de usuarios • Control de acceso a redes • Control de acceso a SO • Control de acceso a aplicaciones • Computación móvil

Adquisición, desarrollo y mant. de sistemas	2, 4, 5	Asegurar que la seguridad es parte integral en los sistemas de información	• Requerimientos de seguridad • Procesamiento correcto de aplicaciones • Controles criptográficos • Seguridad de los sistemas de archivos • Seguridad en los procesos de desarrollo y soporte
Manejo de incidentes	2, 4, 5	Asegurar que los eventos de seguridad de la información y las debilidades asociadas con los sistemas de información son comunicados de manera que permita acciones correctivas en tiempos adecuados.	• Manejo de Incidentes
Gestión de la continuidad del negocio	2, 4, 5	Contrarrestar las interrupciones de las actividades de negocio y proteger los procesos críticos del negocio de los efectos de fallas mayores o desastres en los sistemas de información y asegurar que se reinicien en tiempos adecuados	• Gestión de la Continuidad del Negocio
Compromisos legales	2, 4, 5	Evitar fallas en el cumplimiento de leyes, estatutos, obligaciones reguladoras o contractuales y cualquier requerimiento de seguridad	• SUDEBAN • Cumplir con políticas, estándares y procedimientos • Auditorias internas y externas
Certificación internacional	5	Identificar las instituciones que han pasado por procesos de certificaciones internacionales y su relación con el estado de los fundamentos teóricos	
Organización internacional	4	Identificar los Bancos pertenecientes a la Banca Comercial y Universal que pertenecen a organizaciones internacionales y su relación con el estado de los fundamentos teóricos	

Las variables del presente trabajo de investigación forman los Fundamentos Teóricos en Seguridad de la Información, según la cual se evaluará su desarrollo en la Banca Comercial y Universal de Venezuela; son extraídas de Mejores Practicas" en Seguridad de la Información, en la Tabla 29, se muestra la relación entre las variables de la investigación, el marco teórico, los dominios del CISSP (CBK) y la norma técnica para Seguridad de la Información ISO 17799:2005.

Tabla 29. Relación de las variables con mejores prácticas

Variable	Relación Marco Teórico	CISSP CBK	ISO17799
Gestión Riesgo Informático	Practicas en Seguridad de la Información	Seguridad de la Información y Gestión del Riesgo	Gestión y Tratamiento del Riesgo
Políticas, estándares y procedimientos	Practicas en Seguridad de la Información	Seguridad de la Información y Gestión del Riesgo	Políticas de Seguridad de la Información
Clasificación de la información	Practicas en Seguridad de la Información	Seguridad de la Información y Gestión del Riesgo	Clasificación y Control de los Bienes
Seguridad física y ambiental		Seguridad Física	Seguridad Física y Ambiental
Seguridad en RRHH	Practicas en Seguridad de la Información	Seguridad de la Información y Gestión del Riesgo	Seguridad en RRHH
Gestión de comunicaciones y operaciones		Telecomunicaciones y Seguridad en Redes/Seguridad en Operaciones	Gestión de Comunicaciones y operaciones
Control de acceso		Control de Acceso	
Adquisición, desarrollo y mantenimiento de sistemas	Seguridad en el desarrollo de sistemas y aplicaciones	Seguridad en las Aplicaciones	Mantenimiento de Sistemas y Aplicaciones
Manejo de Incidentes	Incidentes y leyes	Leyes, Regulaciones, Cumplimiento e Investigación	Manejo de Incidentes de Seguridad de la Información
Gestión de la continuidad del negocio	Planificación de Continuidad del Negocio y Recuperación de Desastres	Continuidad de Negocio y Recuperación de Desastres	Planificación de la Continuidad del Negocio
Compromisos legales	Incidentes y leyes	Leyes, Regulaciones, Cumplimiento e Investigación	Cumplimiento

Instrumento de Recolección de Datos

Para desarrollar un instrumento de recolección de datos se debe tomar en cuenta la técnica a emplear, o sea, el procedimiento o forma particular de obtener datos o información.

Al determinar en orden de ideas, la técnica a emplear para el trabajo dependiendo del tipo y diseño de la investigación es la encuesta desarrollada en forma de cuestionario, este se deriva a partir de:

- Definición nominal de las variables.
- Relación con los objetivos de la investigación
- Objetivo de las variables
- Definición operacional de las variables.
- Nivel de medición.

En la Tabla 28, se puede ver la definición de las variables y en la Tabla 29, se puede apreciar la relación de las variables con las mejores prácticas en Seguridad de la Información. El cuestionario está formado por una pregunta única con relación a las variables definidas en la Tabla 28, organizando las respuestas según una escala de Likert.

Debido a la sensibilidad del tema, el cuestionario fue enviado y recibido con la seguridad establecida de mutuo acuerdo y posteriormente contactando la persona vía telefónica para aclarar dudas e información respecto al cuestionario.

El cuestionario entregado se basa en la norma internacional ISO17799:2005 y el CBK del CISSP de ISC2, el cual hace referencia a las normas a seguir en Seguridad de la Información, ver cuestionario en Apéndice A.

Confiabilidad y Validez del Cuestionario

La validez se refiere al grado en que un instrumento realmente mide la variable que pretende medir. Para determinar esta característica pueden tomarse en cuenta diferentes tipos de evidencias relacionadas con el contenido (pertinencia), el criterio (adecuación) o el constructo (redacción).

En la presente investigación se realizó la validez mediante el juicio de expertos (profesionales relacionados con la temática que se investiga), a quienes previamente se les suministró la información del estudio, copia del instrumento y el formato para registrar su opinión acerca de la correspondencia y pertinencia de las preguntas con los aspectos que se mencionan y a la vez se obtuvieron sugerencias y recomendaciones para mejorar el instrumento. La validez de la investigación y su aprobación llevada a cabo por el juicio de expertos se puede evidenciar en el Apéndice A.

La confiabilidad se calculó a través del coeficiente Alfa de Cronbach, y este se llevó a cabo a partir de la aplicación del instrumento. El coeficiente de confiabilidad de alfa de Cronbach resultó 0,9811 ($F = 23,953$; $p = 0,001$) en términos estadísticos se considera un índice excelente, esto quiere decir que la consistencia entre los términos de los ítems evaluados respecto del aspecto de conocimiento indagado es altamente favorable lo que indica que el instrumento reproduce lo que mide; el análisis de

coeficiente de correlación intraclase (para verificar variación dentro de cada sujeto y entre ellos) también resultó significativo, en este caso, el coeficiente referido a la medida simple (intrasujetos) fue altamente significativo (r = 0,5973; IC-95%: 0,4176-0,8134; p = 0,001) en el caso de la medida promedio (intersujetos) el valor del coeficiente fue (r = 0,9811; IC-95%: 0,9617-0,9935; p = 0,001). El instrumento de recolección de información presentado en esta oportunidad muestra alta fiabilidad respecto al esquema de medición propuesto.

Técnicas para el Análisis de los Datos

Una vez trascritos los datos, se codificaron los resultados usando funciones estadísticas de la herramienta de software Microsoft Excel, para describir los valores obtenidos en cada variable. Se uso la estadística simple para aplicar a la codificación. Los resultados se presentan en forma tabulada y gráfica.

Procedimiento

El procedimiento seguido para realizar el Trabajo de Grado de Maestría fue el siguiente:

1. Aplicar el instrumento diseñado.
2. Medir la validez y confiabilidad.
3. Codificar, tabular y graficar los resultados de la aplicación del instrumento, como se describe en las "Técnicas para el análisis de los datos".
4. Analizar los resultados.
5. Generar conclusiones y recomendaciones.

CAPÍTULO IV

RESULTADOS, CONCLUSIONES Y RECOMENDACIONES

Resultados

Para el estudio del cuestionario se tomaron en cuenta cada uno de los puntos analizados durante el trabajo, relacionados entre las mejores practicas según el ISO 27001 y el CBK del CISSP de ISC2; permitiendo mostrar la evaluación del estado, según los expertos de cada institución la situación, de los fundamentos teóricos en Seguridad de la Información.

Para iniciar la exposición de los resultados, se presenta a continuación (ver Figura 18) la representación porcentual de las instituciones pertenecientes a la muestra, que respondieron, se negaron y las que no dieron respuesta al instrumento:

Figura 18. Resultados de la Aplicación del Instrumento

Fuente: Elaboración Propia.

De la muestra de catorce instituciones financieras pertenecientes a la Banca Comercial y Universal de Venezuela respondieron el cuestionario el 86% (12), 7% (1) se negó por considerar que es información confidencial y el 7% (1) restante no respondió.

Los resultados de la aplicación del instrumento se muestra para cada una de las variables, en el caso de las que posean índices, se presenta el resultado de cada uno de ellos ya que se consideran importantes en el contexto de evaluación de la variable.

Para todas las variables incluidas en el instrumento, lo que se midió fue el nivel de avance de esa variable en la organización, con el fin de indagar en relación a la evaluación de la aplicación de los fundamentos teóricos de la seguridad de la información. El primer ítem corresponde al Desarrollo de la Gestión del Riesgo Informático, los resultados fueron los siguientes (ver Figura 19):

Figura 19. Distribución por nivel de Desarrollo en la Gestión del Riesgo Informático. Fuente: Elaboración propia.

Se encuentra entonces que en las instituciones encuestadas el 47% considera que hay un "Suficiente" desarrollo en la gestión del riesgo informático mientras que el 33% lo estima en un nivel de "Bastante", el 17% en "Medio", y solo un 8% cree que se encuentra "Completamente" desarrollado.

La segunda variable corresponde al desarrollo de las Políticas, Estándares y Procedimientos de la organización, los resultados se pueden observar en la Figura 20:

Figura 20. Distribución por nivel de Desarrollo de Políticas, Estándares y Procedimientos.

Fuente: Elaboración propia.

En atención a los resultados obtenidos se puede establecer que en un 41% se considera que esta variable se encuentra suficientemente desarrollada mientras que un 25% la estima completa y un 17%, aprecia que el Desarrollo de Políticas, Estándares y Procedimientos está en un nivel de progreso de poco o bastante. Se puede señalar entonces que por lo menos todas las instituciones han avanzado en el desarrollo de políticas, estándares y procedimientos en relación al riesgo informático.

La tercera variable analizada en el cuestionario está referida al desarrollo de la Organización de la Seguridad Informática, cuyos resultados se presentan en la Figura 21:

Figura 21. Distribución por nivel de Desarrollo de la Organización de la Seguridad Informática.

Fuente: Elaboración propia.

Se puede señalar entonces que el 51%, considera que la organización esta suficientemente desarrollada, mientras que el 33% estiman que esta completamente y el 8% en un nivel de bastante o medio con 8%.

La cuarta variable, se refiere al desarrollo de la Seguridad Física y Ambiental, y sus resultados se muestran a continuación (ver Figura 22):

Figura 22. Distribución por nivel de Desarrollo de la Seguridad Física y Ambiental. Fuente: Elaboración propia.

El 33% aprecia que está bastante desarrollada la Seguridad Física y Ambiental, el 25% lo estima en un nivel "Medio", 25% "Completo", 17% "Suficiente.

La quinta variable está relacionada con el desarrollo de la Clasificación de la Información, los resultados se pueden apreciar en la Figura 23:

Figura 23. Distribución por nivel de Desarrollo de la Clasificación de la Información. Fuente: Elaboración propia.

En este ítem, el 33% valora el nivel de desarrollo como "Medio" mientras que un 25% "Suficiente", 17%, "Poco" o "Bastante" 17% y solo un 8% cree que esta completamente desarrollado.

La variable ubicada en el sexto ítem corresponde con el desarrollo de la Seguridad en Recursos Humanos, con los resultados en la Figura 24:

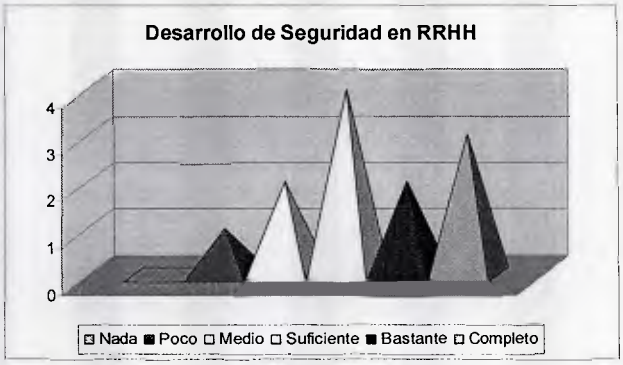

Figura 24. Distribución por nivel de Desarrollo de la Seguridad en Recursos Humanos.

Fuente: Elaboración propia.

Para el caso del desarrollo de la Seguridad en RRHH, los porcentajes obtenidos fueron 33% "Suficiente", 25% "Completo", 17% "Medio" y "Bastante", 8% "Poco".

La séptima variable corresponde a la Gestión de Comunicaciones y Operaciones, comprende los siguientes índices y resultados:

El primer índice corresponde con el Desarrollo del Control de Cambios, cuya aplicación se muestra a continuación (ver Figura 25):

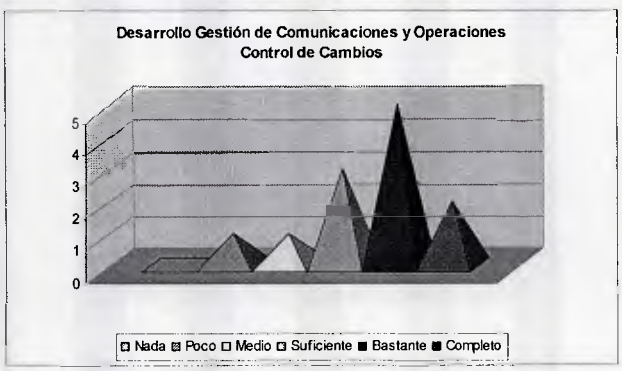

Figura 25. Distribución por nivel de Desarrollo en Control de Cambios.

Fuente: Elaboración propia.

De acuerdo a las instituciones entrevistadas en control de cambios el 42% se encuentra en un nivel bastante desarrollado, mientras que el 25% considera que esta "Suficiente", 17% "Completamente", 8% "Poco" o "Medio" y sin resultados para "Nada".

En la Figura 26 se pueden visualizar los resultados para el segundo índice:

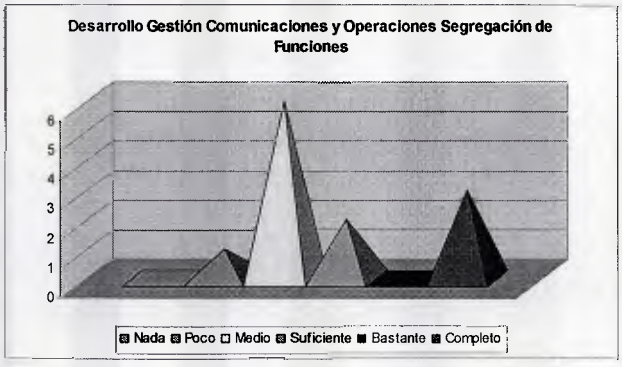

Figura 26. Distribución por nivel de Desarrollo en Segregación de Funciones.
Fuente: Elaboración propia.

Un 50% cree que tiene un desarrollo medio en segregación de funciones, el 25% lo estima "Completo", 17% "Suficiente" y un , 8% "Poco", por ultimo 0% "Nada" y "Bastante".

El índice que corresponde con la Separación Desarrollo y Producción se presenta de la siguiente manera (ver Figura 27):

Figura 27. Distribución por nivel de Desarrollo en la Separación de Desarrollo y Producción.
Fuente: Elaboración propia.

En este caso el 50% estima que esta completamente desarrollada la Separación de Desarrollo y Producción, un 25% "Medio", el 17% "Bastante", 8% "Suficiente", 0% para "Nada" y "Poco". El cuarto índice se indica en los resultados de la Figura 28 a continuación:

Figura 28. Distribución por nivel de Desarrollo en Gestión de Servicios de Terceros.
Fuente: Elaboración propia.

El desarrollo en Gestión de Servicios de Terceros es considerado para un 32% de la muestra en un nivel de "Bastante", el 17% "Poco", "Medio", "Suficiente", "Completo" y 0% para "Nada".

El quinto índice se identifica con el desarrollo de la Planificación y Aceptación de Sistemas, dando los resultados que se señalan en la Figura 29:

Figura 29. Distribución por nivel de Desarrollo en Planificación y Aceptación de Sistemas.
Fuente: Elaboración propia.

En cuanto al nivel de desarrollo área este índice el 34% lo estima en "Suficiente", un 33% "Bastante", 17% "Completo", 8% para "Poco" y "Medio". De acuerdo a esto, la planificación y aceptación de sistemas está en un 67% en un nivel de suficiente o bastante desarrollado.

El sexto índice corresponde al desarrollo de Protección Contra Código Malicioso, se muestra en la Figura 30:

Figura 30. Distribución por nivel de Desarrollo en Protección Contra Código Malicioso.

Fuente: Elaboración propia.

Un 42% valora este nivel de desarrollo en "Suficiente", 33% lo ubica como "Completamente", 17% en medio y el 8% en "Bastante" 8%, y por ultimo "Nada" y "Poco" con 0%.

El séptimo índice se corresponde con el desarrollo de Respaldos o "Backups", los resultados se pueden ver en la Figura 31:

Figura 31. Distribución por nivel de Desarrollo en Respaldos.

Fuente: Elaboración propia.

El nivel de desarrollo para este índice se considera en "Completo", para un 42%, "Suficiente en un 33% de las instituciones", 17%"Bastante", 8% "Medio".

El octavo índice se muestra en la Figura 32,

Figura 32. Distribución por nivel de Desarrollo en Gestión de la Seguridad en Redes.
Fuente: Elaboración propia.

El Desarrollo en Gestión de la Seguridad en Redes se considera para la muestra encuestada en bastante para el 50%, suficiente en un 25%, mientras que el 17% lo estima en "Completamente" y 8% "Medio".

El índice del noveno ítem revisa el desarrollo de la Manipulación de Medios, los resultados se pueden observar en la Figura 33:

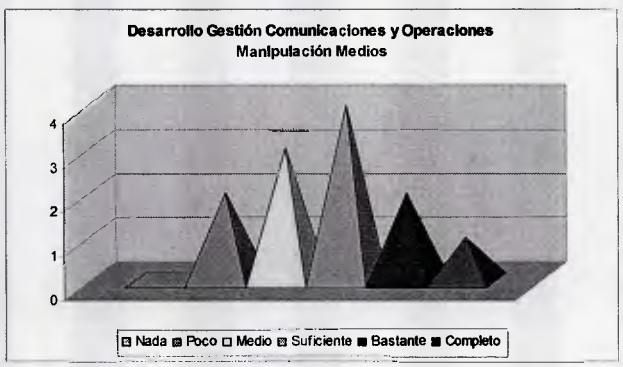

Figura 33. Distribución por nivel de Desarrollo en la Manipulación de Medios.
Fuente: Elaboración propia.

El nivel de Desarrollo en la Manipulación de Medios se estima en "Suficiente" para el 33% seguida de 25% "Medio", 17%"Poco" y "Bastante", 8% "Completo".

El décimo índice se relaciona en la Figura 34:

Figura 34. Distribución por nivel de Desarrollo en Intercambio de Información.
Fuente: Elaboración propia.

El 25% considera que el desarrollo de intercambio de información de su institución se encuentra uniformemente entre un nivel de "Medio", "Suficiente", "Bastante" y "Completamente".

Los resultados obtenidos para el décimo primer índice se muestran en la Figura 35:

Figura 35. Distribución por nivel de Desarrollo en Servicios de Comercio Electrónico.
Fuente: Elaboración propia.

En este índice el 34% estima que el desarrollo en Servicios de Comercio Electrónico de su institución se encuentra en un nivel suficiente mientras que el 33% lo ubica en "Bastante", 25% en "Completamente" y el 8%, en "Nada".

El último índice en la variable de desarrollo de la Gestión de Comunicaciones y Operaciones tiene que ver con el índice desarrollo del Monitoreo y Control, el resultado se puede observar en la Figura 36:

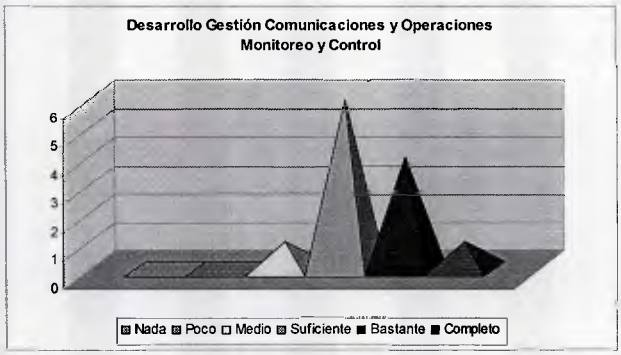

Figura 36. Distribución por nivel de Desarrollo en Monitoreo y Control.
Fuente: Elaboración propia.

El 51% considera "Suficiente" la medida de desarrollo de este índice el ,33% lo estimó en "Bastante" mientras que un 8% considera que en su institución se encuentra en un nivel "Medio" o "Completo".

La siguiente variable del instrumento corresponde al Desarrollo del Control de Acceso, esta se encuentra subdividida en cinco índices, que se presentan a continuación:

En la Figura 37 se puede observar el resultado del primer índice, el cual está relacionado con el desarrollo de la Gestión de Acceso de Usuarios:

Figura 37. Distribución por nivel de Desarrollo en Gestión de Acceso de Usuarios.
Fuente: Elaboración propia.

El 33% de las organizaciones pertenecientes a la muestra respondió que el desarrollo de este índice es "Bastante" o "Completo", el 17% considera que en su institución se encuentra en un nivel "Medio" o "Suficiente". Este resultado muestra positivamente la adhesión que deben llevar las instituciones con la mejor práctica de "Need to Know" abordada a lo largo de este trabajo de investigación.

Los resultados obtenidos para el segundo índice de esta variable se presentan en la Figura 38:

Figura 38. Distribución por nivel de Desarrollo en Control de Acceso a Sistemas Operativos.

Fuente: Elaboración propia.

El nivel del Desarrollo en Control de Acceso a Sistemas Operativos se estimó que se encuentra para un 33% en un nivel de "Bastante" o "Completamente" mientras que el 17% cree que está en "Medio" o "Suficiente".

En el tercer índice se tiene el desarrollo de Control de Acceso a Redes, presentando los resultados en la Figura 39:

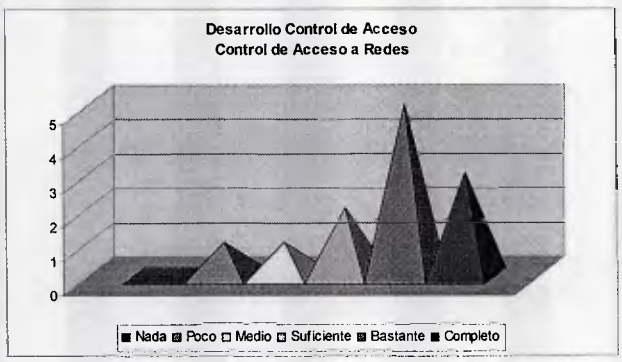

Figura 39. Distribución por nivel de Desarrollo en Control de Acceso a Redes.

Fuente: Elaboración propia.

Para un 42% el Desarrollo en Control de Acceso a Redes se encuentra en un nivel de "Bastante" desarrollada, el 25% lo ubica en "Completamente", el 17% en "Suficiente", y un 8% en "Poco" o "Medio".

Los resultados de la Figura 40 que se presentan a continuación indican el nivel de Desarrollo en Control de Acceso a Aplicaciones según los encuestados:

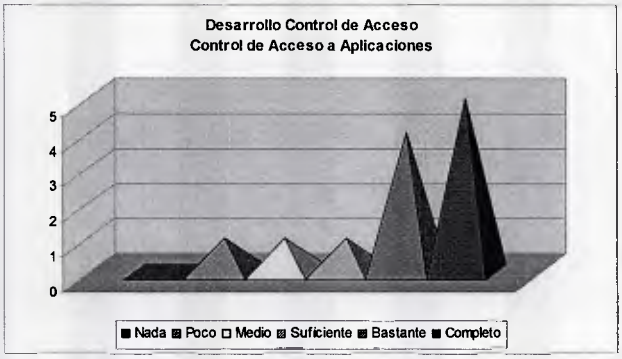

Figura 40. Distribución por nivel de Desarrollo en Control de Acceso a Aplicaciones.
Fuente: Elaboración propia.

Encontrando que para un 43% esta ubicado en un nivel completo de desarrollo en su institución mientras que para un , 33% esta Bastante desarrollado y un 8% considera que esta "Poco", "Medio" o "Suficientemente " respectivamente.

El último índice se presenta en la Figura 41:

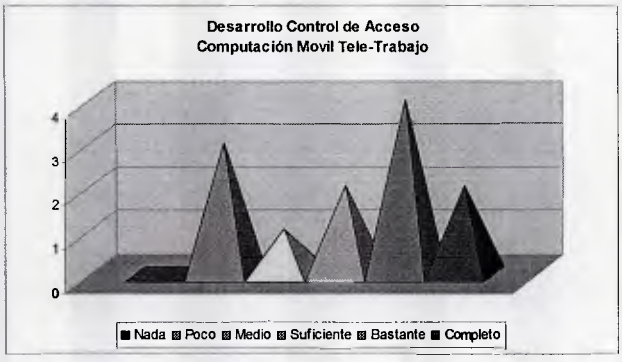

Figura 41. Distribución por nivel de Desarrollo en Computación Móvil y Tele-Trabajo.
Fuente: Elaboración propia.

El desarrollo de Control de Acceso para el caso de la computación móvil y teletrabajo se ubica para un 33% como "Bastante, el 25% considera que está "Poco" desarrollado y el ,17% "Suficiente" o "Completo", finalizando con 8% "Medio".

En el ítem de la novena variable se encuentra el nivel de desarrollo en la Adquisición, Desarrollo y Mantenimiento de Sistemas de Información, el cual está compuesto por cinco índices:

La Figura 42 muestra los resultados del primer índice que corresponde al desarrollo en Requerimientos de Seguridad:

Figura 42. Distribución por nivel de Desarrollo en Requerimientos de Seguridad.
Fuente: Elaboración propia.

Para un 33% este índice se encuentra en un nivel de "Suficiente" desarrollo, el 25% "Bastante" o "Completo" y un 17% ubica el desarrollo de este índice en su institución en una fase "Medio".

En el segundo índice se presenta el desarrollo de Procesamiento Correcto de Aplicaciones, los resultados se pueden observar en la Figura 43:

Figura 43. Distribución por nivel Desarrollo Procesamiento Correcto de Aplicaciones.
Fuente: Elaboración propia.

Las respuestas en este índice fueron bastante homogéneas encontrándose que un 25% de los encuestados ubicaría el nivel de Desarrollo en Procesamiento Correcto de Aplicaciones en su institución en niveles de "Medio", "Suficiente", "Bastante" y "Completo", sin encontrar resultados para las medidas "Nada" y "Poco".

El desarrollo de Controles Criptográficos viene dado en el tercer ítem correspondiente a la variable Adquisición, desarrollo y mantenimiento de sistemas de información, la muestra arrojó el resultado ilustrado en la Figura 44:

Figura 44. Distribución por nivel de Desarrollo en Controles Criptográficos.
Fuente: Elaboración propia.

El 42% de las instituciones encuestadas ubica este índice en un nivel de "Bastante" desarrollado mientras que un 25% considera que está "Completo", el 17% "Poco" adelantado y el 8% cree que esta en una fase de "Medio" o "Suficiente" progreso.

El cuarto índice viene dado por el desarrollo de la Seguridad en los Sistemas de Archivos, y sus resultados se pueden observar en la Figura 45:

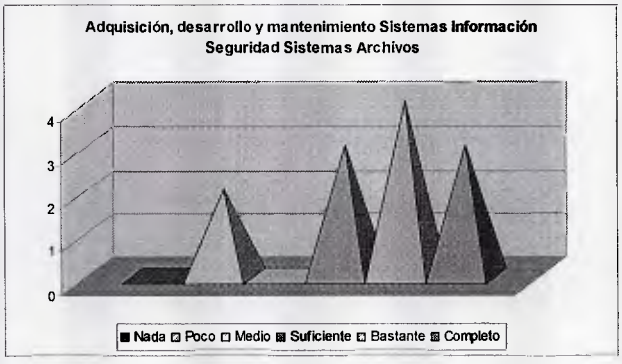

Figura 45. Distribución por nivel Desarrollo en Seguridad de Sistemas de Archivos.
Fuente: Elaboración propia.

El Desarrollo en Seguridad de Sistemas de Archivos se considera en una etapa de "Bastante" progreso para un 33%, en tanto que para un 25% está en un nivel de "Suficiente" o "Completamente" y para un 17% tiene "Poco desarrollo en su institución.

Para finalizar esta variable se presenta el desarrollo de la Seguridad en los Procesos de Desarrollo y Soporte, arrojando los siguientes resultados (ver Figura 46):

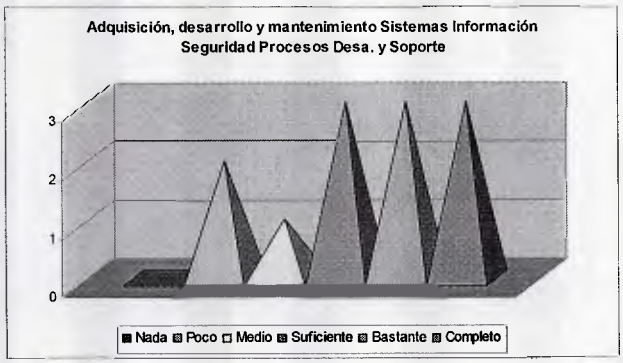

Figura 46. Distribución por nivel de Desarrollo en Seguridad de Procesos de Desarrollo y Soporte.

Fuente: Elaboración propia.

Para un 25% el nivel de desarrollo de este índice en su organización se encuentra en niveles de Suficiente", "Bastante" y "Completo" indistintamente y un 17% ubica su institución con "Poco" progreso y el 8% en una etapa "Media".

En la Figura 47 se muestran los resultados de la aplicación del instrumento a la variable Desarrollo del Manejo de Incidentes:

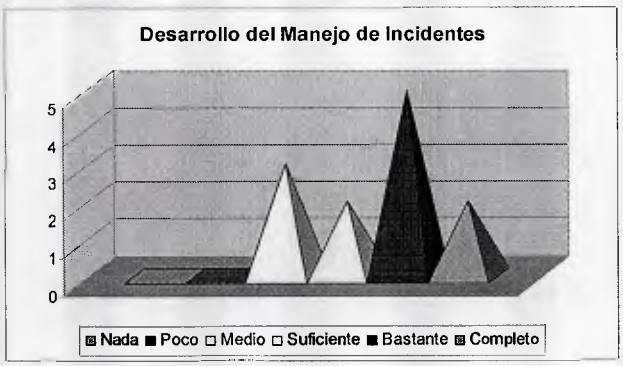

Figura 47. Distribución por nivel de Desarrollo en Manejo de Incidentes.

Fuente: Elaboración propia.

Las personas encuestadas consideran que en cuanto al Desarrollo en Manejo de Incidentes sus instituciones se ubican en un nivel de "Bastante" el 25% piensa que está en "Medio desarrollo y para el 17% sitúa a su organización en etapas de progreso de "Suficiente" y "Completamente".

El desarrollo en la Gestión de Continuidad del Negocio es la variable décimo primera, cuyos resultados se presentan a continuación (ver Figura 48):

Figura 48. Distribución por nivel de Desarrollo en Gestión de Continuidad del Negocio.

Fuente: Elaboración propia.

Para este índice se encontró que el 25% de las personas encuestadas consideran que sus instituciones se encuentran indistintamente en niveles de "Medio", "Suficiente" y "Completo" de desarrollo en tanto que un 17% ubicaría su organización en una etapa de "Bastante" progreso y el 8% en "Poco".

El Desarrollo de Compromisos Legales es la última de las variables presentadas en el cuestionario y esta compuesta por tres índices que se muestran a continuación:

El primer índice corresponde con el desarrollo de compromisos legales dictados por SUDEBAN, los resultados se indican a continuación (ver Figura 49):

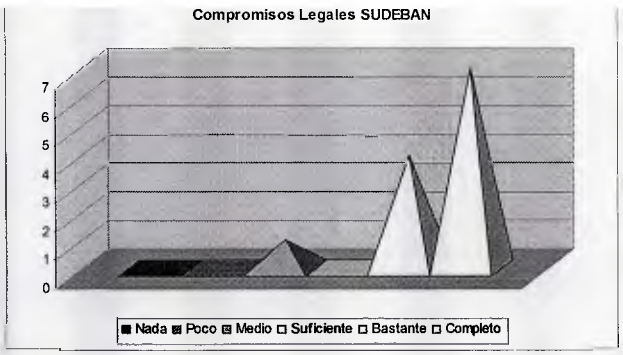

Figura 49. Distribución por nivel de Desarrollo de Compromisos Legales – SUDEBAN.

Fuente: Elaboración propia.

El 59% de las instituciones identifican su nivel de desarrollo en las regulaciones establecidas por SUDEBAN como "Completo", el 33% en "Bastante", un 8% en "Medio" y 0% para "Nada", "Poco" y "Suficiente".

El segundo índice corresponde al desarrollo del Cumplimiento de Políticas, Estándares y Procedimientos, los porcentajes obtenidos se pueden observar en la Figura 50:

Figura 50. Distribución por nivel de Desarrollo en Cumplimiento de Políticas, Estándares y Procedimientos.

Fuente: Elaboración propia.

Para el 34% se considera que el nivel de Desarrollo en Cumplimiento de Políticas, Estándares y Procedimientos es "Suficiente" en tanto que el 33% cree que esta

"Bastante" desarrollado, un 25% lo estima "Completo" y el 8% en una etapa "Medio".

El ítem del cuestionario perteneciente a la variable Compromisos Legales corresponde al desarrollo de Auditorias Internas y Externas, la Figura 51 presenta los resultados obtenidos:

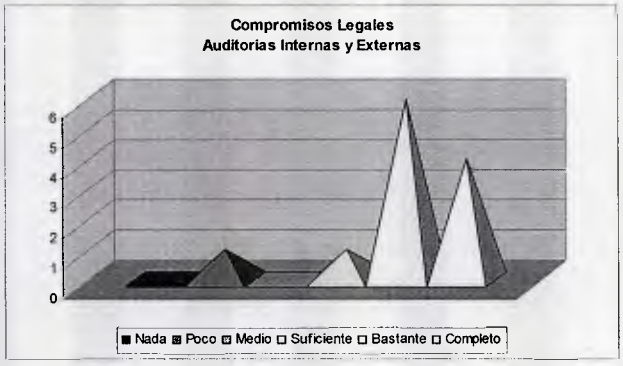

Figura 51. Distribución por nivel de Desarrollo en Auditoria Interna y Externa.

Fuente: Elaboración propia.

Para este último ítem se mostró que el 51% de las personas encuestadas consideran que sus instituciones se encuentran "Bastante" comprometidas con las auditorías internas y externas, 33% se encuentran "Completamente", 8% "Suficientemente" comprometidas y el 8% restante "Poco".

La variable correspondiente a la pertenencia de la Banca Comercial y Universal de Venezuela a organizaciones internacionales reportó los resultados mostrados en la Figura 52:

Figura 52. Pertenencia de la Banca Comercial y Universal a organizaciones internacionales.

Fuente: Elaboración propia

Para esta variable las organizaciones pertenecientes a empresas trasnacionales se ubicó en 58% mientras que las nacionales se ubicaron en 42%

Los resultados de la variable final del estudio correspondiente con Certificación Internacional ISO se pueden observar en la Figura 53:

Figura 53. Cumplimiento de Normas Internacionales Tipo ISO.

Fuente: Elaboración Propia.

Las organizaciones pertenecientes a la Banca Comercial y Universal que cumplen Certificaciones Internacionales tipo ISO se ubicaron en un 17% y las que no en un 83%.

Conclusiones

1. Se analizaron los Fundamentos Teóricos en Seguridad de la Información basados en la norma técnica ISO17799:2005 y el cuerpo teórico de la certificación Profesionales de Seguridad en Sistemas de Información (CISSP), encontrando que:
   - La mayoría de los Bancos Comerciales y Universales de la muestra objeto de este estudio se encuentran en una etapa de desarrollo de la aplicación de los Fundamentos Teóricos entre bastante y completamente.
   - Las variables referidas a Seguridad de la Información en el aspecto técnico tales como Controles de Acceso, Gestión de Comunicaciones y Operaciones, y Seguridad Física y Ambiental se encuentran en su mayoría en los niveles bastante y completamente.
   - Las variables referidas a Seguridad de la Información en el aspecto de gestión como es el caso de Gestión del Riesgo Informático, Políticas, Estándares y Procedimientos, Clasificación de la Información y Gestión Continuidad Negocio se encuentran en los niveles medio y completamente.
   - Las variables referidas a Adquisición, desarrollo y mantenimiento de sistemas se ubicaron en su mayoría en niveles bastante y completamente.
   - Las variables correspondientes a los compromisos legales se ubicaron en los niveles bastante y suficiente.
   - Se encontró que el ítem Respaldos perteneciente a la variable Gestión de Comunicaciones y Operaciones se encuentra más desarrollado que la variable Clasificación de la Información.
   - Se encontró que el ítem Cumplir Políticas, Estándares y Procedimientos se encuentra más desarrollado que la variable Desarrollo de Políticas, Estándares y Procedimientos
2. Se planteó un ciclo de Seguridad de la Información el cual comprende los Fundamentos Teóricos plasmados en este trabajo y la relación entre sus

componentes con el fin de facilitar la gestión de la Seguridad de la Información en la Banca Comercial y Universal.

3. Se conocieron las mejores prácticas en Gerencia de Seguridad de la Información entre las cuales se encuentran:
   - Marco de Seguridad de la Información.
   - Políticas, Estándares y Procedimientos.
   - Gerencia del Riesgo Informático.
   - Buenas prácticas en Seguridad de la Información: Clasificación de la Información, Rotación de Trabajo, Separación de Funciones, Need to Know, Prácticas de Contratación, Terminación, Due Care y Due Diligence.
4. Se estudiaron las bases de Seguridad de la Información en el Desarrollo de Sistemas y Aplicaciones, el cual debe ser aplicado por las gerencias respectivas en las organizaciones para generar aplicaciones seguras.
5. Se determinaron los Planes de Continuidad de Negocio y Recuperación de Desastres utilizados como mejores prácticas los cuales la Banca Comercial y Universal deben aplicar para cumplir con la Normativa impuesta por SUDEBAN.
6. Se identificaron las leyes venezolanas relacionadas con Seguridad de la Información hallándose que la legislación actual contempla de manera amplia el tema.
7. Se situó el estado de aplicación de los Fundamentos Teóricos en Seguridad de la Información encontrándose mucha fuerza en el desarrollo técnico y con respecto a la parte de gestión y gerencia indicios de desarrollo pero sin el mismo avance que la parte técnica.
8. Se identificó que los Bancos Comerciales y Universales que poseen certificaciones como ISO se encuentran mejor desarrollados en la aplicación de los Fundamentos Teóricos en Seguridad de la Información.
9. Se apreció que los Bancos Comerciales y Universales pertenecientes a empresas multinacionales se encuentran en niveles de desarrollo de la aplicación de los Fundamentos Teóricos entre Bastante y Suficiente en la mayoría de las variables, salvo casos de organizaciones que se están estableciendo en el país.

Recomendaciones

1. De acuerdo a los resultados obtenidos en la aplicación del instrumento y relacionando los fundamentos teóricos en Seguridad de la Información, se considera pertinente realizar futuras investigaciones en los siguientes aspectos:
    a. Iniciar estudios en las organizaciones venezolanas de la Banca Comercial y Universal respecto a su madurez en Seguridad de la Información.
    b. El ciclo de Seguridad de la Información y su aplicación para ayudar en la Gestión de la Seguridad de la Información en las organizaciones.
    c. Metodologías más ajustadas a la Gestión del Riesgo Informático y su aplicación.
    d. La utilización de recursos en las organizaciones si la aplicación del ítem Respaldos perteneciente a Gestión de Comunicaciones y Operaciones está más desarrollado que la variable Clasificación de la Información es importante estudiar la utilización de recursos en las organizaciones.
    e. Analizar la aplicabilidad de las leyes relacionadas con Seguridad de la Información a la realidad venezolana.
    f. Determinar el perfil y capacitación requeridos por el personal involucrado con Seguridad de la Información.
    g. Formas y estrategias para aumentar el desarrollo de la Manipulación de Medio.
2. Con base en los resultados obtenidos es importante que las organizaciones objeto de la presente investigación se enfoquen en mejorar el ámbito de gestión ya que el ambito técnico se está cubriendo adecuadamente.
3. Aplicar la Seguridad de la Información en el desarrollo de aplicaciones y sistemas, ya que al disminuir la vulnerabilidad de los sistemas el riesgo informático será menor.

4. Concientizar a la alta dirección de las organizaciones para que tomen decisiones basadas en el conocimiento generado por sus recursos y mejores prácticas en el mercado.
5. Entrenar constantemente al personal involucrado en Seguridad de la Información ya que las vulnerabilidades detectadas en sistemas y aplicaciones, y los mecanismos de control suelen ser muy dinámicos.
6. Concientizar a los directivos de la organización en relación a que la Seguridad de la Información en las organizaciones abarca un panorama más amplio que factores técnicos y que todos deben estar correctamente atendidos.
7. Dirigir el esfuerzo de las organizaciones que requieran aumentar la aplicación del desarrollo en Seguridad de la Información a obtener certificaciones tipo la norma técnica ISO 17799:2005.

REFERENCIAS BIBLIOGRÁFICAS

(Asobanca,2005) Asociación Bancaria de Venezuela. (2007). *Evolución del sistema financiero venezolano*. Extraído en Junio 2007 del sitio web de la Asociación bancaria nacional: http://www.asobanca.com.ve/bancos.asp?id=8#

(Barge,2002) Barge, Bill. (2002). *C-I-A Security Triad.* Extraído en Mayo 2008 del sitio web de la Universidad Tri-State:
http://www.tristate.edu/faculty/barge/cs103/C-I-A%20Security%20Triad.html

Boehm, Barry (1981). *Software Engineering Economics Software Engineering Economics* (1981) November 1981, NJ, USA.

(BSA,2007). Business Software Alliance. (2007). *La Tasa de Piratería de Software Para Computadoras Personales Bajo Dos Puntos Porcentuales en Latinoamérica en el 2006 a 66%.* Extraído en Febrero 2008 del sitio Web de Business Software Alliance:http://w3.bsa.org/latinamerica-spanish/press/newsreleases/2007-global-piracy-study.cfm.

Caralli, Richard (2004) *The Critial Success Factor Method: Establishing a Foundation for Enterprise Security Management.* Extraído del sitio Web de la Universidad de Carnegie Mellon, Instituto de Ingeniería de Software en Octubre 2008:
http://www.sei.cmu.edu/publications/documents/04.reports/04tr010/04tr010.html

(Código civil venezolano) Congreso Nacional. (1982). *Código Civil.* Gaceta Oficial N° 2.990. Caracas – Venezuela.

Comité de Supervisión Bancaria de Basile (2004). *Aplicación de Basilea II: aspectos prácticos.* Extraído del sitio Web del Banco de Pagos Internacionales en Octubre 2008: http://www.bis.org/publ/bcbs109esp.pdf

(Constitución Nacional) Asamblea Nacional Constituyente. (2000). *Constitución de la República Bolivariana de Venezuela.* Gaceta Oficial N° 5.453. Caracas – Venezuela.

(Decreto con Fuerza de Ley de Reforma de la Ley General de Bancos y otras Instituciones Financieras) Asamblea Nacional. (2001). *Decreto con Fuerza de Ley de*

Reforma de la Ley General de Bancos y otras Instituciones Financieras. Gaceta Oficial N° 5.555. Caracas - Venezuela

(DRI,2006) DRII & DRJ. (2006) *Generally accepted practices for business continuity practicioners*. Disaster Recovery Institute International & Disaster Recovery Journal.

(Echenique,2004) Echenique, J. (2004). *Implantación de una red privada virtual (VPN) para el acceso seguro y controlado al sistema de información del sector eléctrico venezolano.* Trabajo de grado para optar al título de especialista en Telecomunicaciones. Facultad de Ingeniería. Universidad Central de Venezuela. Caracas, Venezuela.

(Elnacional,2007) Guia.com.ve (2007). *Crimen cibernético tiene más ganancias que el tráfico de drogas*. Extraído en Febrero 2008 del sitio Web de guia.com.ve: http://www.guia.com.ve/noticias/?id=14626

(Entrust,2006) Entrust. (2006). Entrust *custom partner training*. Ontario, Canada: Entrust.

(Fowler,2003) Fowler, S. *Information classificaiton – who, why and how*. Extraído en Febrero 2006 del sitio web del Sans Institute: http://www.sans.org/reading_room/whitepapers/auditing/846.php

(Grance,2004) Grance, T., Hash, J. & Stevens, M. (2004). *Security Considerations in the information system development life cycle*. Gaithersburg, MD: NIST Special Publication.

(Guldentops,2004) Guldentops, E. (2004). *The IT Dimensiono f Basel II.* Information systems audit and control association/Information systems control journal, volume 6.

(Peñaloza,2005) Peñaloza, A. (2005). *Notas de clases*. Notas de clases Seminario I y II de la Universidad Católica Andrés Bello, Caracas, Venezuela.

(Hamana,2003) Hamana, J. (2003). *Elementos básicos para modelos de seguridad en organizaciones venezolanas*. Trabajo de grado para optar al título de Magíster en Gerencia de Sistemas. Decanato de Estudios de Postgrado. Universidad Metropolitana. Caracas, Venezuela.

(Hansche,2004) Hansche, S., Berti, J. & Hare, C. (2004). *Official ISC2 guide to the CISSP exam*. Boca Ratón, FL: Auerbach/CRC Press LLC.

(Harris,2003) Harris, S. (2003). *CISSP all in one exam guide (2da. Edición)*. Emerville, CA: McGraw Hill/Osborne.

(Hernandez,2003) Hernández, R., Fernández, C. & Baptista, P. (2003). *Metodología de la investigación (3ra. Edición)*. DF México Mc Graw Hill.

(Hiles,2004) Hiles, A. (2004). *Business continuity: Best practices (2da. Edición)*. Disaster Recovery Institute/Business Continuity Institute.

(IEEE,1993) IEEE. (1993). *IEEE software engineering standard: Glossary of software engineering terminology*. Extraído en mayo del 2005 del sitio web de la IEEE: http://www.ieee.org/portal/site

(INTERPOL,2008) INTERPOL. (2008,Mayo) Informe Forense de INTERPOL sobre los Ordenadores y Equipos Informáticos de las FARC Decomisados por Colombia. Extraído en Junio del 2008 del sitio web de INTERPOL: http://www.interpol.int

(ITGI,2007) IT Governance Institute. (2007). *IT control objectives for basel II – The importante of governance and risk management for compliance*. Rolling Meadows, IL: IT Governance Institute.

(ISO/IEC15408,1998) ISO/IEC. (1998). *Information technology – security techniques – evaluation criteria for it security ISO/IEC 15408*. International Organization for Standardization.

(ISO/IEC17799,2005) ISO/IEC. (2005). *Information technology – security techniques – code of practice for information security management*. International Organization for Standardization.

(IWS,2008) Internet World Stats. (2008, Mayo 15). *Internet Usage Statistics*. Extraído en Mayo 2008 del sitio web de Internet World Statistics: http://www.internetworldstats.com/stats.htm.

(Keele,2005) Keele, A. & Mortier, K. (2005). *CISA exam cram 2*. QUE Publishing.

(Krutz,2003) Krutz, R & Vines, R. (2003). *The CISSP prep guide (Gold Edition)*. Indianapolis, Indiana: Prentice Hall.

(Ley Especial Contra Delitos Informáticos) Asamblea Nacional. (2001*). Ley Especial Contra Delitos Informáticos*. Gaceta Oficial N° 37.313. Caracas – Venezuela.

(Ley de Mensajes de Datos y Firmas Electrónicas) Asamblea Nacional. (2001). *Ley de Mensajes de Datos y Firmas Electrónicas*. Gaceta Oficial N° 37.148. Caracas - Venezuela

(Ley Orgánica de Identificación) Asamblea Nacional. (2006). *Ley Orgánica de Identificación*. Gaceta Oficial N° 38.458. Caracas – Venezuela.

(Ley para la protección de Niños, Niñas y Adolescentes en Salas de Uso de Internet, Videojuegos y otros Multimedia) Asamblea Nacional. (2006). *Ley para la protección de Niños, Niñas y Adolescentes en Salas de Uso de Internet*. Gaceta Oficial N° 38.529. Caracas – Venezuela.

(Mendehall,1981) Mendehall, Reinmuth (1981). *Estadística para Administración y Economía*. California USA. Editorial Wadsworth International.

(Microsoft,2006) Microsoft Corporation. (2006). *The security risk management guide*. San Francisco, CA: Microsoft Corporation.

(MSU,2007) Disaster recovery planning team. (2007). *Disaster recovery planning*. Extraído del sitio web de la Universidad de Michigan: http://www.drp.msu.edu/Planning.htm

(Northcutt,2003) Northcutt, S. (2003). Computer security incident handling. USA. Sans Press.

(OWASP,2005) OWASP. (2005). *A guide to building secure web applications and web services. (2.0 Black Hat Edition)*. Extraído en Noviembre 2006 del sitio web de Open Web Application Security Pproject: http://www.owasp.org

(Palazzolo,2008) Palazzolo, Maria Gracias. (2008, Marzo). *Audiencias Digitales en Venezuela*. Extraído en Mayo 2008 del sitio web de Cavedatos: http://www.cavedatos.org.ve/download/cdt_655.pps

(Perera,2005) Perera, Tom (2005). *Enigma Cipher Machines, Fialka, Nema, Other Cipher Machines, Antique Computers and Calculators*. Extraído en Mayo del 2008 del sitio Web de W1TP Museum: http://w1tp.com/enigma/

(Pittol,2004) Pittol, M. (2004). *Evaluación de seguridad de una institución financiera mediante la ejecución de un estudio de penetración interno y externo a su infraestructura tecnológica*. Trabajo de grado para optar al título de Especialista en

Telecomunicaciones. Facultad de Ingeniería. Universidad Central de Venezuela. Caracas, Venezuela.

(RAE,2006)) Real Academia Española. (2006). *Diccionario de la lengua española.* Extraído en Junio 2007 del sitio web de la Real Academia Española: http://www.rae.es/

Royce, Winston W. (1970): *Managing the Development of Large Software Systems: Concepts and Techniques. In: Technical Papers of Western Electronic Show and Convention (WesCon)* August 25-28, 1970, Los Angeles, USA.

(RNV,2007) Prensa Web Radio Nacional de Venezuela/Ultimas Noticias. *Banca debe prepararse para combatir fraude electrónico*. Extraído en Febrero 2008 del sitio Web del Centro Nacional de Tecnologías de Información:

http://www.cnti.gob.ve/cnti_docmgr/detalle.html?categoria=5429

(RNVAN,2007) Prensa Web Radio Nacional de Venezuela/Asamblea Nacional. *Asamblea Nacional en pie de lucha contra la pornografía infantil*. Extraído en Febrero 2008 del sitio Web del Ministerio del Poder Popular para la Comunicación e Información: http://www.rnv.gov.ve/noticias/index.php?act=ST&f=2&t=47149

(Rodriguez,2004) Rodriguez, M. (2004). *Estudio de técnicas biométricas para verificación de identidad en sistemas de control de acceso*. Trabajo de grado para optar al título de Especialista en Telecomunicaciones. Facultad de Ingeniería. Universidad Central de Venezuela. Caracas, Venezuela.

(Sans,2001) Guel, Michele D. *A short primer for developing security policies*. Extraído en Agosto 2005 del sitio web de Sans Institute: http://www.sans.org/resources/policies/

(Shirey,2000) Shirey, R. *RFC 2828 internet security glossary*. Extraído en Febrero 2006 del sitio web del IETF: http://www.ietf.org/rfc/rfc2828.txt

(Skoudis,2005) Skoudis, E. (2005). *Incident handling step-by-step and computer crime investigation*. USA. Sans Institute.

(SORM,2006) SORM. (2006). *Business Continuity Impact Analisys*. Extraído en Abril de 2006 del sitio web del state office risk management: http://www.sorm.state.tx.us/Risk_Management/Business_Continuity/bus_impact.php

(Stallings,2006) Stallings, W. (2006). *Cryptography and network security principles and practices (4ta. Edición)*. Upper Saddle River, NJ: Prentice Hall.

(Stoneburner,2002) Stoneburner, G., Goguen, A. & Feringa A. (2002). *Risk management guide for information technology systems*. Falls Church, VA: NIST Special Publication.

(Swanson,2002) Swanson, M., Wohl, A., Pope, L., Grance, T., Hash, J. & Thomas, R. (2002). *Contingency planning guide for information technology systems*. Washington, DC: NIST Special Publication.

(Tablante,2001) Tablante, Carlos (2001). *Delitos Informáticos delincuentes sin rostro*. Caracas: EnCambio.

(Tendenciasdigitales,2006) Tendencias Digitales. (2006). *Venezolanos compraron por Internet un total de US$ 132.000.000 al cierre del 2005*. Extraído en Febrero 2008 del sitio Web de Tendencias Digitales:
http://www.tendenciasdigitales.com/detalle.aspx?id=29&plantilla=1

(Tipton,2002) Tipton, H. & Krause, M. (2002). *Information security management handbook*. CRC Press LLC.

(Unionradio,2006) Unión Radio. (2006). *Mercado venezolano inundado en el 85% por audiovisuales piratas*. Extraído en Febrero 2008 del sitio Web del Centro Nacional de Tecnologías de Información:
http://www.cnti.gob.ve/cnti_docmgr/detalle.html?categoria=3396

(Vitti,2003) Vitti, N. (2003). *Diseño e implementación de una WAN segura para el Instituto Nacional de Estadística (INE)*. Trabajo de grado para optar al título de Especialista en Telecomunicaciones. Facultad de Ingeniería. Universidad Central de Venezuela. Caracas, Venezuela.

(Wheeler,2003) Wheeler, D. (2003). *Secure programming for linux and unix howto*. Boston, MA: GNU Free Documentation License

APÉNDICE A

Marque con una equis "X" como esta desarrollada su organización en factores que influyen en la Seguridad de la Información.

A continuación un ejemplo:

	Nada					Totalmente
Manejo de Incidentes					X	

Si usted considera que su organización se encuentra bastante desarrollada en el manejo de incidencias de seguridad coloca la **X** cerca de totalmente

Factores		**Nada**					**Totalmente**
	Gestión Riesgo Informático						
	Políticas, estándares y procedimientos						
	Organización de la Seguridad Informática						
	Clasificación de la información						
	Seguridad Física y ambiental						
	Seguridad en RRHH						
Gestión de comunicaciones y operaciones	Control de Cambios						
	Segregación de funciones						
	Separación desarrollo y producción						
	Gestión servicios 3ros.						
	Planificación y aceptación sistemas						
	Protección contra código malicioso						
	Respaldos o "Backup"						
	Gestión seguridad redes						
	Manipulación de medios						
	Intercambio de información						
	Servicios de comercio electrónico						
	Monitoreo y control						
Control de acceso (CA)	Gestión de acceso de usuarios						
	Control de acceso a redes						
	CA sistemas operativos						
	CA a aplicaciones						
	Computación móvil tele trabajo						
Adquisición desarrollo y mantenimiento sistemas Información	Requerimientos de seguridad						
	Procesamiento correcto de aplicaciones						
	Controles criptográficos						
	Seguridad de los sist. de archivos						
	Seguridad procesos desarrollo y soporte						
	Manejo de incidentes						
	Gestión Continuidad Negocio						
Compromisos legales	SUDEBAN						
	Cumplir políticas estándares procedimientos						
	Auditorias internas y externas						

En las preguntas a continuación responda si o no:

Pertenece su empresa a una organización internacional?

Posee su organización alguna certificación reconocida internacionalmente como ISO?

APÉNDICE B

Validación de Expertos

Caracas, Octubre 2007

ACEPTACIÓN

Por medio de la presente, acepto como válido el instrumento presentado ante mí por el Lic. Juan Carlos Palacios, tanto en pertinencia, criterio y redacción; el juicio realizado por mí persona correspondió con el ámbito metodológico. La aplicación de este instrumento es con fines netamente académicos.

Sin otro particular a que hacer referencia,

Atentamente,

3751885

Prof. Soledad Díaz Heredia

C.I 3.751.885

Universidad Metropolitana

0412625933