PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

FACULTAD DE INGENIERÍA

TESIS PREVIA A LA OBTENCION DEL TITULO DE MAGISTER EN GERENCIA DE TECNOLOGÍAS DE LA INFORMACIÓN

"ANÁLISIS COSTO/BENEFICIO DE LA APLICACIÓN DEL ESTÁNDAR ISO/IEC 27001:2005 EN UNA EMPRESA INDUSTRIAL EN LA PROVINCIA DE PICHINCHA"

VANESSA HURTADO MOLINA

EDWIN PATRICIO ARIAS CRUZ

DIRECTOR: ING. JAVIER CÓNDOR

REVISORES: ING. ALBERTO PAZMIÑO

ING. ROBERTO UNDA

Quito DM., 2012-MAYO

AGRADECIMIENTOS

Agradecemos a nuestros revisores de Tesis: Alberto Pazmiño y Roberto Unda y

A nuestro Director Javier Cóndor.

Vanessa Hurtado Molina

Un agradecimiento especial a mi familia por su infinito apoyo y

a mi compañero de Tesis Patricio Arias,

Por su paciencia, buen ánimo y motivación a lo largo del ciclo académico y en el desarrollo de la presente Tesis.

Edwin Patricio Arias Cruz

A la empresa que me ha permitido ampliar mis conocimientos:
ACERIA DEL ECUADOR CA ADELCA.

A mi compañera de Maestría y Tesis:

Vanessa,

por su capacidad, perseverancia y esfuerzo.

DEDICATORIA

Vanessa Hurtado Molina

Dedicado a mi madre Consuelo Molina Rubio,

a mi padre Roberto Hurtado Gomezjurado,

a mi hermano Roberto Francisco Hurtado Molina y

a mi novio Andrés Santiago Utreras Escobar

Sin su apoyo, constante motivación y comprensión,

Este logro no hubiese sido posible

Edwin Patricio Arias Cruz

Este trabajo está dedicado a mi familia:

Ana Lucía, Paúl, Danny y Gaby,

por su constante estímulo y comprensión.

Gracias a ustedes,

hoy puedo ver alcanzada una nueva meta.

TABLA DE CONTENIDOS

AGRADECIMIENTOS I
DEDICATORIA II
INTRODUCCIÓN 1
CAPÍTULO I: LA INFORMACIÓN COMO RECURSO ESTRATÉGICO DE LAS EMPRESAS 3
1.1. Las empresas en la era de la Información 3
1.2. La Información como recurso estratégico 4
CAPÍTULO II: LA SEGURIDAD DE LA INFORMACIÓN 7
2.1. Concepto de la Seguridad de la Información 7
2.2. Elementos de la Seguridad de la Información 8
2.2. Importancia de la Seguridad de la Información 10
2.3. Situación actual de la Seguridad de la Información en Latinoamérica 14
2.3.1. Resultados Encuesta de la Seguridad de la Información en Latinoamérica 14
2.4. Estándares de Seguridad de la Información 18
2.4.1. Estándar RFC2196 19
2.4.2. Estándar IT Baseline Protection Manual 22
2.4.3. Estándar SSE-CMM 24
2.4.4. Estándar ISO/IEC 17799[B] 25
2.4.5. Estándar ISO/IEC 27001[J] 27
2.5. Evaluación de estándares de seguridad de la información 28
CAPÍTULO III: ESTÁNDAR ISO/IEC 27001:2005 30
3.1. Introducción al estándar ISO/IEC 27001:2005[J] 30
3.2. Contenido del estándar ISO/IEC 27001:2005[J] 33
3.3. Beneficios de la aplicación del estándar ISO/IEC 27001:2005[J] 36
3.4. Costo de implementación del estándar ISO/IEC 27001:2005[J] 37
3.5. Aplicación de la ISO/IEC 27001:2005[J] 40
3.6. Certificación de la ISO/IEC 27001:2005[J] 44
3.6.1. FASE 1: Revisión de la documentación: 44
3.6.2. FASE 2: Auditoría “in situ” 45
CAPÍTULO IV: PROCEDIMIENTO PARA EL ANÁLISIS COSTO BENEFICIO 47
4.1. Fases para el análisis Costo Beneficio 47
4.2. Visión general de la seguridad de información en la empresa seleccionada 51

4.3. Recopilación de información sobre activos de información de la empresa 51
4.4. Evaluación de Riesgos cualitativa y cuantitativa 55
4.4.1. Evaluación de Riesgos Cualitativa 55
4.4.2. Evaluación de Riesgos Cuantitativa 63
CAPÍTULO V: VISION GENERAL DE LA SEGURIDAD DE LA INFORMACIÓN EN LA EMPRESA SELECCIONADA 69
5.1. Historia de la empresa 69
5.2. Información estratégica de la empresa 69
5.3. Descripción del negocio y sector empresarial 71
5.4. Situación actual de la seguridad de la información en la empresa 75
CAPÍTULO VI: ANÁLISIS COSTO BENEFICIO DE LA APLICACIÓN DEL ESTÁNDAR ISO/IEC 27001:2005 A LA EMPRESA INDUSTRIAL SELECCIONADA .. 79
6.1. Recopilación de información sobre activos de la información de la empresa 79
6.2. Evaluación de Riesgos Cualitativa 88
6.3. Evaluación de Riesgos Cuantitativa 105
CAPÍTULO VII: CONCLUSIONES Y RECOMENDACIONES 117
7.1. Conclusiones 117
7.2. Recomendaciones 122
BIBLIOGRAFÍA Y REFERENCIAS 124
GLOSARIO DE TERMINOS 127
INDICE DE FIGURAS 130
INDICE DE CUADROS 131
INDICE DE ANEXOS 134

INTRODUCCIÓN

La dinámica del mundo empresarial obliga a las organizaciones a tomar decisiones inmediatas basadas en fuentes oportunas y confiables. Una de ellas, que se va constituyendo en elemento clave de la estrategia organizacional, es la información; y la consecución e interpretación para que ésta sea un componente de soporte al entorno gerencial, requiere de un aliado fundamental, que es la tecnología. Los continuos aparecimientos de vulnerabilidades en los sistemas de información, noticias de accesos no deseados e incluso debilidades manifiestas en software ampliamente extendido y crítico para el funcionamiento de las empresas, hacen de la seguridad de la información un área de especial atención para el correcto desarrollo de los negocios en esta actual era digital. Interesa a todos disponer de un entorno de confianza en el que las empresas puedan desarrollar, mantener y extender sus modelos de negocio. Es el tiempo donde importa la seguridad de los negocios de los clientes.

El presente trabajo busca como objetivo principal demostrar el costo beneficio de la aplicación de la normativa ISO/IEC 27001:2005[J] en el entorno de la información de una empresa industrial, partiendo de su situación actual y el efecto en el nivel de riesgo de la empresa luego de la aplicación de la norma. La diferencia a favor o en contra de la organización nos dará información para evaluar su costo beneficio.

La evaluación de riesgos requiere de un proceso formal para identificar y asignar prioridades a los riesgos en la organización, para lo cual se ha seleccionado la Guía de Administración de Riesgos de Seguridad de Microsoft[1], metodología que facilita su medición cualitativa y cuantitativa dentro de la organización. Esta guía ayuda a planear, crear y mantener un programa de administración de riesgos de seguridad, mediante un proceso dividido en cuatro fases:

1. Evaluación del riesgo: La fase de evaluación del riesgo nos permitirá determinar el beneficio entre la inversión económica realizada y los niveles de seguridad que se proyectarían con la aplicación del estándar ISO/IEC 27001:2005[J].

[1] Microsoft Technet, *Guía de Administración de riesgos de seguridad*: http://www.microsoft.com/spain/technet/recursos/articulos/srsgch03.mspx Acceso: marzo 2012

2. Apoyo a la toma de decisiones: identificar y evaluar las soluciones de control según un proceso definido de análisis de costo-beneficio.
3. Implementación de controles: implementar y poner en funcionamiento las soluciones con el fin de reducir el riesgo para la empresa.
4. Medición de la efectividad del programa: analizar la efectividad del proceso de administración de riesgos y comprobar que los controles proporcionan el nivel de protección previsto.

Para cumplir con los objetivos específicos propuestos, el presente trabajo se ha distribuido en siete capítulos de la siguiente manera:

El primero es una introducción al entendimiento de la información como recurso estratégico en las empresas, exponiendo las razones que motivaron nuestro estudio.

En el segundo capítulo se presenta una visión general de la Seguridad de la Información, los conceptos principales necesarios para comprender la teoría y los estándares utilizados para mantener un control sobre los riesgos, justificando la elección de la ISO/IEC 27001:2005[J] como estándar a aplicar en el cálculo del costo beneficio del presente trabajo.

El tercer capítulo presenta el estándar ISO/IEC 27001:2005[J], a fin de percibir su alcance y volumen.

En el cuarto capítulo se establece la teoría que define el procedimiento empleado para el análisis costo beneficio.

En el quinto capítulo se describe el negocio de la empresa seleccionada y se establece una visión general en cuanto a seguridad de la información.

En el sexto se presenta el análisis costo beneficio de la implementación de la norma, proporcionando información útil para el apoyo a la toma de decisiones sobre acciones adecuadas para mitigar los riesgos identificados, siguiendo el procedimiento propuesto en el cuarto capítulo. La evaluación de riesgos, en conjunto con herramientas de costos como el cálculo del Retorno de la Inversión en Seguridad (ROSI), nos permitirá determinar el beneficio entre la inversión económica realizada y los niveles de seguridad que se proyectarían con la aplicación del estándar ISO/IEC 27001:2005.

Por último, la tesis culmina en las conclusiones, recomendaciones y líneas de investigación.

CAPÍTULO I: LA INFORMACIÓN COMO RECURSO ESTRATÉGICO DE LAS EMPRESAS

En las empresas, los recursos financieros, materiales y humanos constituyen ejes claves para su gestión. En este entorno, además del capital, la tierra y el trabajo, aparece la información como un nuevo recurso a gestionar. En un mundo cada vez más complejo y cambiante, la necesidad por información es cada vez más apremiante. Este capítulo presenta un análisis del aporte que brinda la información acompañada de tecnología a la estrategia de una empresa, al ambiente que rodea a la gerencia para facilitar el proceso de toma de decisiones y la realización eficaz de las funciones de planeación, control y operaciones.

1.1. Las empresas en la era de la Información

La Era de la Información o Sociedad del Conocimiento como la denomina el conocido "padre de la Administración", Peter Drucker, nos brinda la idea de que en la actualidad las personas tenemos la capacidad de libremente transferir información y tener acceso instantáneo a los conocimientos que anteriormente habrían sido difíciles o imposibles de encontrar. La Era de la Información se apoya en un paradigma tecnológico en el que son imprescindibles los ordenadores y la informática, las telecomunicaciones y la microelectrónica. Es en este nuevo entorno tecnológico en donde la información aumenta su valor económico, facilita el mejoramiento de los procesos productivos y estimula la introducción de nuevos bienes y servicios. Una empresa moderna se adelanta a sus competidores, es proactiva en sus decisiones; para lo cual demanda información de carácter estratégico**.**

De acuerdo con Peter Drucker, "No hay ninguna duda de que éste es el momento de hacer el futuro, precisamente porque todo está cambiando. Ahora es el tiempo para la acción" [2]

Complementando con las palabras del Gurú del Marketing Philip Kotler, "Lo más importante es pronosticar hacia dónde van a ir los competidores, y estar ahí antes que ellos" [3] (Kotler, Phillip)

[2] Drucker,Peter, *La sociedad poscapitalista*, Buenos Aires, Editorial Sudamericana, 1993

No queda duda que la llamada Revolución de la Información**,** asociada a un cambio tecnológico, sin precedentes, permite que los canales y medios por los cuales se maneja y transfiere, hayan dinamizado su producción, distribución y uso de manera incuestionable, haciendo posible y potenciando un efecto globalizador.

1.2. La Información como recurso estratégico

El uso y administración de la información constituye una necesidad para que las empresas mantengan vigente el conocimiento que requieren para alcanzar sus objetivos, por lo cual la misma constituye un recurso indispensable para la organización. Al ser la información un factor productivo (recurso), es importante gestionarla.

La aplicación de la información a los diferentes procesos organizacionales, trae implícito un cambio en la cultura empresarial, transformaciones en las normas, metodologías y proyección de la organización, incluso ocasionando cambios en sus productos o servicios.

Una vez más citamos a Peter Drucker para evidenciar la importancia de la información: "El saber que hoy consideramos saber se demuestra en la acción: lo que ahora queremos decir con saber, es información efectiva en la acción; información enfocada a resultados." [2]

Según un artículo escrito en la Revista del Empresario Cubano[4], el uso efectivo de la información depende de dos elementos: La tecnología y los contenidos; esto es, la infraestructura tecnológica necesaria y, mediante la utilización de la misma, un tratamiento adecuado de los contenidos. La combinación óptima de estos factores, hace posible que la información de la organización cuente con los atributos necesarios:

- Que sea pertinente, oportuna y eficaz, para influir satisfactoriamente en los resultados de la gestión organizacional.
- Que cumpla con los principios: disponibilidad, confidencialidad e integridad.

[3] Philip Kotler, Marketing Management, New Jersey, Prentice Hall, 2000, página 159.

[4] Aleida Olivé García, "La Información: Un recurso estratégico para las organizaciones", *La Revista del Empresario Cubano* , http://www.betsime.disaic.cu/secciones/tec_enemar_08.htm. Acceso: marzo 2012

Las organizaciones necesitan incorporar la información para:

- La identificación y solución de problemas.
- La toma de decisiones.
- El mantenimiento de su capacidad innovadora.
- El logro de la eficacia, eficiencia y competitividad.

El nivel de información amplía la racionalidad de las decisiones, ya que mientras mejor informado esté el decisor, tomará decisiones más ajustadas a sus necesidades. Una mejor calidad de las decisiones tomadas repercutirá en los niveles de eficacia, eficiencia y competitividad de la organización.

La necesidad de información en las empresas se resume en la figura 1-01, en la cual se puede apreciar cómo ésta es aprovechada por cada nivel organizacional en función del tiempo y su nivel de detalle. Los empleados y mandos medios manejan información en línea y de detalle, la información histórica es de mayor utilidad para los analistas de negocio, en tanto que el nivel ejecutivo la requiere totalizada y en línea.

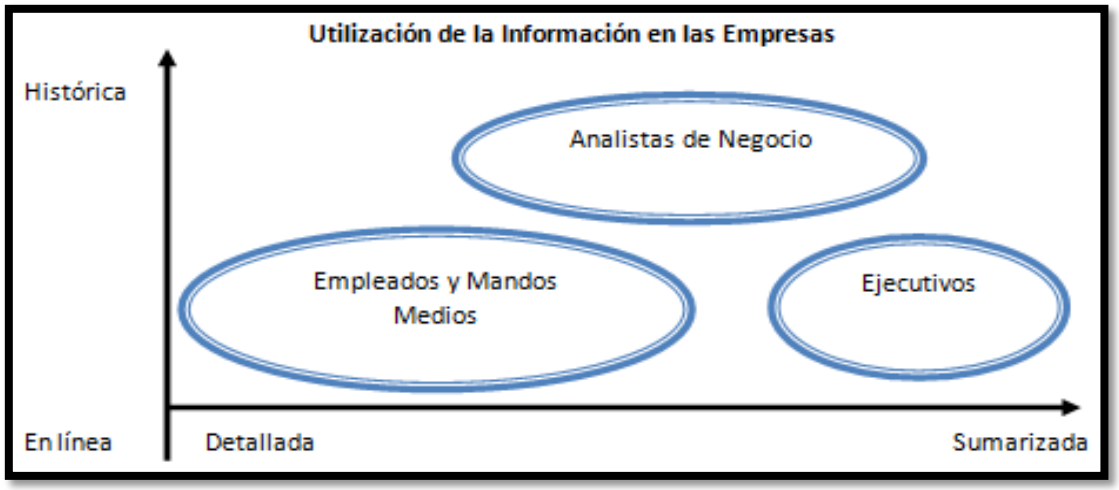


Figura 1-01 Utilización de la Información en las Empresas[A]

Ahora bien, el proceso decisorio requiere y demanda todo tipo de información, tanto interna como externa:

- La información interna se genera dentro de la organización y proporciona la posibilidad de medir su desempeño. Esta puede ser: de Producción, Científica, Tecnológica, Financiera, Comercial, de Recursos Humanos, de Calidad y Legal.

- La información externa se genera fuera de la organización y permite que la empresa se pueda adaptar a su entorno, aprovechando mejor las oportunidades y minimizando las amenazas que puedan presentarse, puede ser: Tecnológica, Comercial, Financiera, Legal, Política, Social o Ambiental.

Según un estudio European Business Communication Survey, realizado por Novell[5], el cual indaga sobre el grado de transparencia informacional en las relaciones internas de la empresa:

- El 45% de los empleados en Europa cree que los conocimientos no se comparten suficientemente en su empresa.
- Un 47% acepta que frecuentemente pierde el tiempo buscando información que con un sistema debidamente organizado podría tener a su alcance fácilmente.
- Otro 43% se queja de no recibir suficiente información por parte de sus directivos.
- El 90% manifiesta que una comunicación efectiva es importante para mantener la moral de los trabajadores.

Si tenemos en cuenta cuánto representa para las organizaciones poder contar con información, no es difícil comprender por qué ésta se ha constituido en un recurso necesario para producir bienes y servicios, tal como anteriormente se encontraban el trabajo, la tierra, el capital y la energía.

[5] Novell, "European Business Communication Survey", *El Profesional de la Información: Revista Internacional Científica y Profesional*, julio 1998, Internet. http://www.elprofesionaldelainformacion.com/contenidos/1998/julio/el_uso_de_la_informacion_en_las_empresas.html Acceso: marzo 2012

CAPÍTULO II: LA SEGURIDAD DE LA INFORMACIÓN

La importancia de la información, convierte a la misma en blanco de ataques, por lo que debe ser protegida y asegurada. Cualquier persona puede querer apropiarse de información útil para obtener un beneficio, ya sea un individuo u otra empresa malintencionada. La información no solo sufre el riesgo de ser divulgada sino de pasar por modificaciones indebidas, ocasionando que ésta deje de ser confiable e íntegra. También puede sufrir de ataques a su disponibilidad, si la información no se encuentra a disposición cuando sea requerida, es como no tenerla. Como menciona la norma ISO/IEC 17799, "la información es un activo, que como otros activos importantes del negocio, tiene valor para la organización y requiere en consecuencia una protección adecuada". [B]

En este capítulo profundizamos en el conocimiento de la Seguridad de la Información, sus conceptos, su situación actual dentro de las empresas y también en el ámbito latinoamericano. Presentamos algunas metodologías existentes y mediante un análisis comparativo se sustenta el estándar de seguridad para la aplicación del costo beneficio del presente proyecto de tesis.

2.1. Concepto de la Seguridad de la Información

El estándar ISO/IEC 17799[B] define a la Seguridad de la Información como: "Preservación de la confidencialidad, integridad y disponibilidad de la información". Estos atributos se definen así:[6]

- Integridad: garantiza que los datos no han sido alterados ni destruidos de modo no autorizado. La información es modificada, incluyendo su creación y borrado, sólo por el personal autorizado.

[B] ISO/IEC 17799 Part 1: Code of practice for information security management

[6] Arturo Grau Barberá, *Introducción a la Protección y Seguridad de la Información*, Internet. http://alarcos.inf-cr.uclm.es/doc/PSI/tema1Marian.pdf Acceso: marzo 2012

- Disponibilidad: garantiza que la información está disponible para los usuarios autorizados cuando la necesiten. Según la metodología de análisis y Gestión de Riesgos de los sistemas de información MAGERIT, la disponibilidad define el "grado en que un dato está en el lugar, momento y forma en que es requerido por el usuario." [C]
- Confidencialidad: Condición que asegura que la información no pueda estar disponible o ser descubierta por o para personas, entidades o procesos no autorizados.

2.2. Elementos de la Seguridad de la Información

La Seguridad de la Información lleva consigo una serie de conceptos importantes para su entendimiento. A continuación se proporcionan los elementos básicos necesarios para la comprensión de la gestión de la Seguridad de la Información[7] [D]:

- Activo de información: Un activo en una empresa es todo bien tangible o intangible que ésta posee que puede producir un beneficio. Los activos de información son aquellos que representan, contienen, almacenan o transmiten información.
- Amenaza: es la probabilidad de ocurrencia de cualquier tipo de evento (incidente) que puede producir un daño (material o inmaterial) sobre los activos de información, en base a los principios de confidencialidad, integridad y disponibilidad de la información.
- Probabilidad de Ocurrencia: Frecuencia con la cual una amenaza puede ocurrir.
- Incidente de Seguridad: Evento con consecuencias negativas que puede comprometer la integridad, disponibilidad y confidencialidad de la información.
- Vulnerabilidad: Conocida a veces como falencias o brechas, representa el grado de exposición a las amenazas en un contexto particular. Las vulnerabilidades están en relación directa con las amenazas, porque si no existe una amenaza, tampoco existe la vulnerabilidad o no tiene importancia, porque no puede ocasionar daño.

[C] MAGERIT, *Gestión de Riesgos de los sistemas de información, Versión 2*, ©MINISTERIO DE ADMINISTRACIONES PÚBLICAS, Madrid, 20 de junio de 2006 (v 1.1)

[7] Proyecto AMPARO-LACNIC, *Manual Fortalecimiento de la Capacidad Regional de Atención de Incidentes de Seguridad en América Latina y el Caribe Internet*, 2012, Internet, http://www.proyectoamparo.net/files/manual_seguridad/manual_sp.pdf, Acceso: marzo 2012

[D] Álvaro Soldano, *Conceptos sobre Riesgo: Síntesis temática realizada para el Foro Virtual de la RIDM creado para la Capacitación para la Teledetección Aplicada a la Reducción del Riesgo por Inundaciones*, Argentina, marzo 2009, página 3.

- Nivel de Exposición: Instancia en la cual un activo de información es susceptible a dañarse por una amenaza. No significa que el evento que produce la pérdida o daño esté ocurriendo si no que podría ocurrir dado que existe una amenaza y una vulnerabilidad.
- Impacto: Consecuencia que produce un incidente de seguridad sobre la empresa debido a las vulnerabilidades que tiene el activo afectado.
- Control, Medida, Salvaguarda o Contramedida: representa todas las acciones que se implementan para prevenir la amenaza. No sólo son soluciones técnicas, sino también reflejan la capacitación y la toma de conciencia por parte de la organización, además de reglas claramente definidas.
- Riesgo: Es la probabilidad de que una amenaza se convierta en un desastre aprovechando una vulnerabilidad. La vulnerabilidad o las amenazas por separado no representan factores de peligro pero si se juntan, se convierten en un riesgo. En función de una ecuación se puede considerar al riesgo como:

Riesgo = impacto (vulnerabilidad) * probabilidad (amenaza)

Integrando los elementos en un solo concepto: La información vista como un activo vital en las organizaciones, puede presentar vulnerabilidades y encontrarse expuesta a amenazas. Las amenazas explotan vulnerabilidades, ocasionando incidentes de seguridad. La probabilidad de ocurrencia y el impacto de un incidente de seguridad determinan un riesgo. Los riesgos pueden ser mitigados mediante la implementación de controles.[7]

A continuación, se presenta un gráfico que representa las interrelaciones entre las variables principales que componen el riesgo (activo, amenaza y vulnerabilidad):

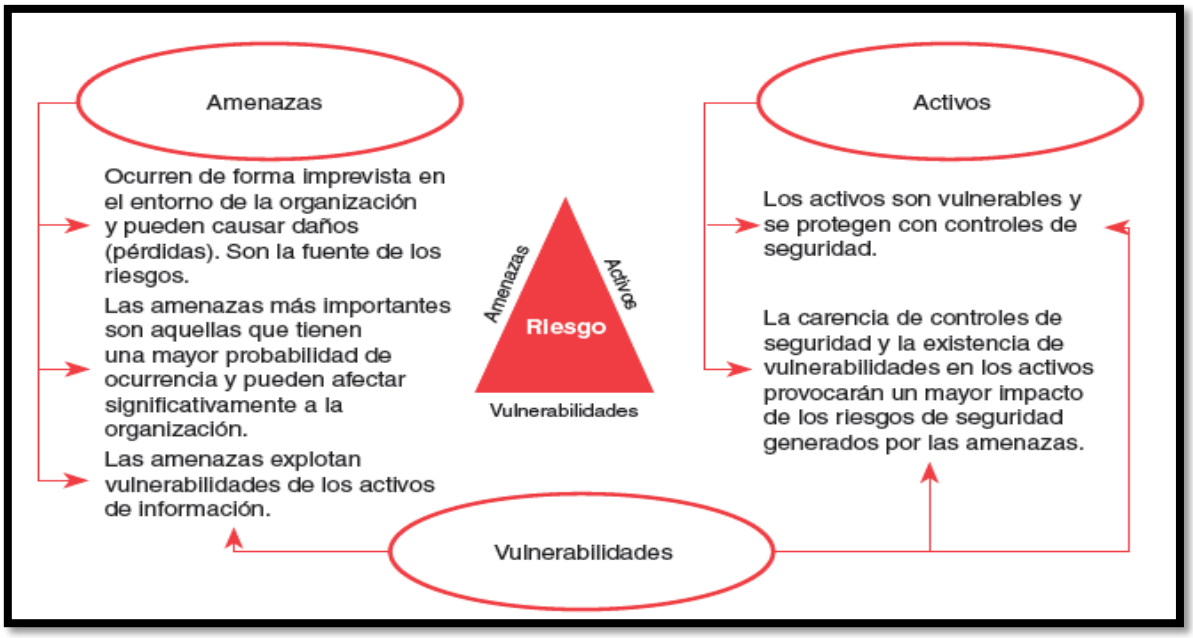


Figura 2-01 Interrelación entre variables principales que componen el riesgo[E]

2.2. Importancia de la Seguridad de la Información

El alcance que denota la importancia de la Seguridad de la Información, según Javier Areitio[F] , se refleja en el siguiente fragmento: "La seguridad de la información es un proceso en el que se da cabida a un creciente número de elementos: aspectos tecnológicos, de gestión-organizacionales, de recursos humanos, de índole económica, de negocios, de tipo legal, de cumplimiento, etc.; abarcando no solo aspectos informáticos y de telecomunicaciones sino también aspectos físicos, medioambientales, humanos, etc."

Existen amenazas reales como una caída de la luz, una inundación, un incendio, un robo, fraudes ayudados por computadora, espionaje, sabotaje y más, que deben ser tratadas de forma preventiva para evitar que las pérdidas sean tan graves que afecten a la viabilidad del negocio. Por esto, es necesario que las empresas establezcan una serie de medidas técnicas, organizativas y procedimentales que garanticen la continuidad de las actividades o procesos de negocio en caso de tener que afrontar una contingencia grave.

[E] Inteco – Deloitte, *Guía para PYMES, Cómo Implantar un Plan de Continuidad del Negocio*, 2010, página 36

[F] Javier Areitio, *Seguridad de la Información, Redes, Informática y Sistemas de Información* , Madrid, España, Paraninfo, 2008, Prólogo.

Son múltiples las empresas que, independientemente de su tamaño, fracasan o incluso desaparecen por la falta de procesos, mecanismos y técnicas que mitiguen los riesgos a los que están expuestas y garanticen una alta disponibilidad en las operaciones de su negocio.[E]

En la figura 2-02, se presentan los resultados sobre el porcentaje de empresas que han experimentado un incidente de seguridad, estudio realizado por el CSI– Computer Crime and Security Survey en el 2010 a profesionales en Estados Unidos[G] :

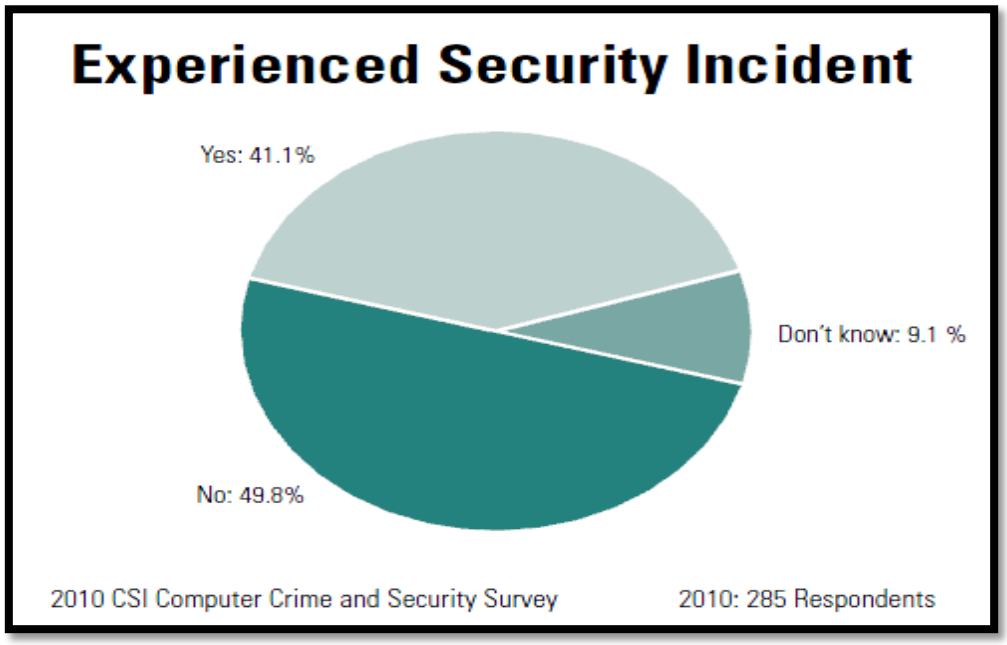


Figura 2-02 Tipos de Ataques Experimentados – Por porcentaje de respuestas[G]

En esta figura, las empresas indican que no han pasando por problemas de seguridad significativos, de hecho la mitad de ellos (49.8%) no experimentó un solo incidente en el periodo de un año que cubrió la encuesta. Sin embargo, cualquier persona con experiencia en el tema conoce que este dato no es porque efectivamente la mitad no tuvieron amenazas si no que seguramente existieron muchas clases de amenazas de seguridad, pero generalmente se tratan de ataques básicos.

El 41.1% de los encuestados confirmaron estar experimentando un ataque a la vulnerabilidad de la seguridad de la información en sus empresas al momento de la encuesta. El 9.1% no tenía conocimiento, lo cual se considera una situación igual de grave.

[G] Robert Richardson, *15th Annual 2010/2011 Computer Crime and Security Survey*, 2011, pág 15.

Continuando con la encuesta mencionada, dentro de los tipos de amenazas que experimentaron incremento de casos registrado, durante el año 2010 están: Infecciones por Malware, Phising y Bots en las redes. La siguiente figura 2-03 refleja los resultados de la encuesta en cuanto a los tipos de ataques experimentados en las empresas[G]:

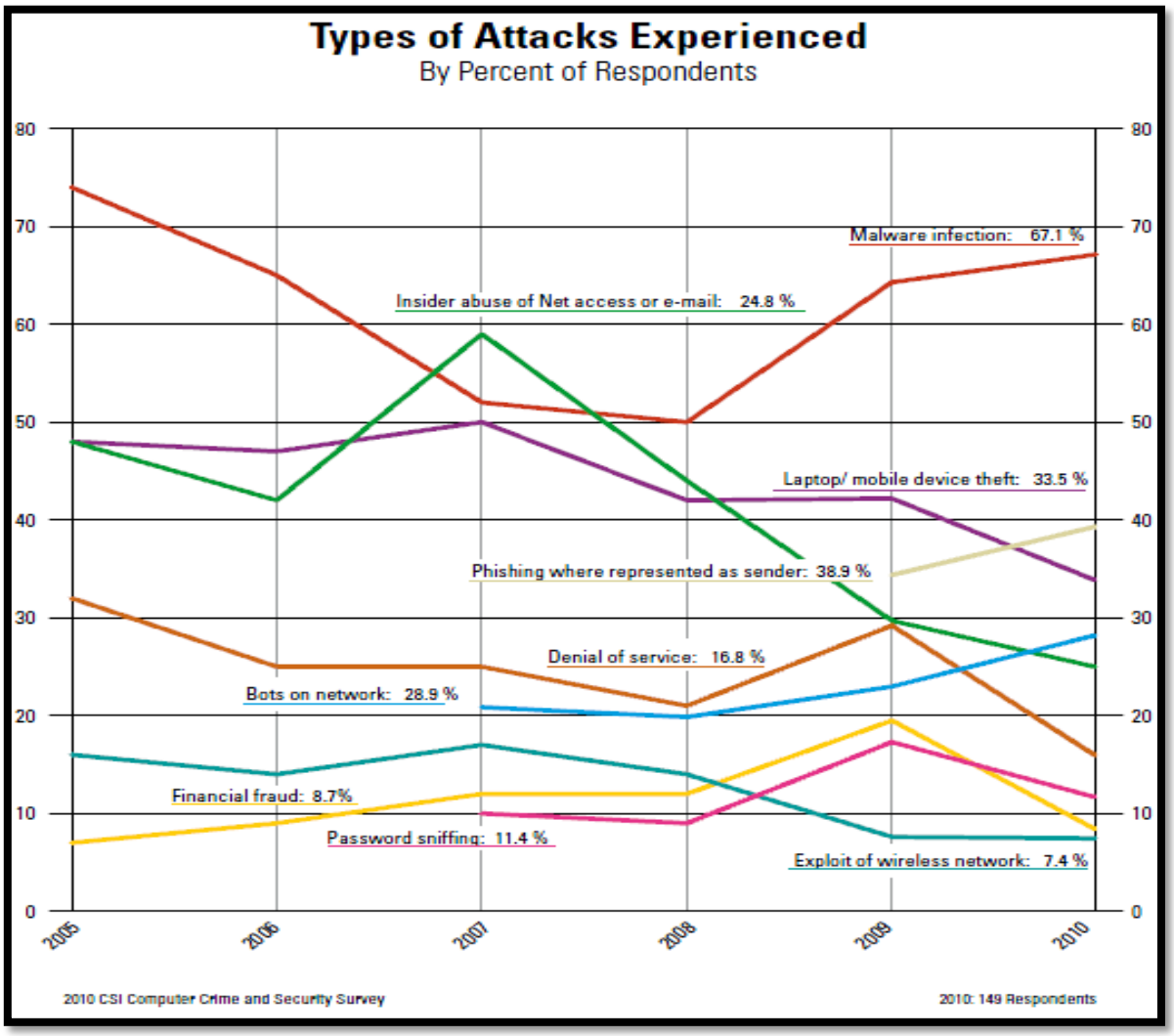


Figura 2-03 Tipos de Ataques Experimentados – Por porcentaje de respuestas[G]

La información previamente mostrada evidencia que no existen sistemas de información totalmente seguros. La seguridad que puede lograrse a través de los medios técnicos es limitada y debe apoyarse en una adecuada gestión de sus procedimientos.

[G] Robert Richardson, *15th Annual 2010/2011 Computer Crime and Security Survey*, 2011, pág 15.

Según datos presentados por la empresa CONISEC-SGSI, dedicada al estudio y soluciones para empresas y certificada en Gestión de Seguridad de la Información[8]:

- El 94% de empresas cerrarían a los dos años de una pérdida severa de la información en sus sistemas.
- El 70% no sobreviviría a más de 4 días sin sus datos. (universidad de Texas)
- La información está sometida a las siguientes amenazas y riesgos (Computer Security Institute)[G]:
    - 55% Error Humano
    - 20% Problemas técnicos
    - 19% Empleados (lucro o intencionalidad)
    - 6% Virus y ataques externos

Según un estudio realizado por Ashish Grag, Jeffrey Curtis y Hilary Halper[9], sobre un total de 22 incidentes de seguridad entre 1996 y 2002, el precio de las acciones de las empresas afectadas cayó un 2,7% el primer día tras conocerse públicamente la noticia, y un promedio del 4,5%, lo que supuso una pérdida media por incidente de 918 millones de dólares (Garg, y otros, 2003). Aunque estos resultados no pueden ser extrapolados a todos los tipos de compañías, son un claro ejemplo del daño causado por un incidente de seguridad medido tan solo en los costes del daño a la imagen corporativa.

Cada vez las empresas están más consientes de la importancia que representa la seguridad de la información, por lo que el definir, mantener y mejorar la seguridad de la información es esencial para conservarse en el borde competitivo, mantener un alto flujo del dinero en efectivo, tener rentabilidad, cumplimiento legal, y sostenimiento de la imagen comercial.

[8] CONISEC-SGSI, *Conectia-Tecnología y Comunicaciones, Propuesta de Servicios*, Internet. http://www.conisec.com/pdf/sgsi-conisec.pdf Acceso: marzo 2012.

[9] David Reinares Lara, *Implantación de la ISO27001: Factores críticos de éxito y visión de la norma como motor de generación de valor añadido*, Innotec System, Internet. http://www.mundointernet.es/IMG/pdf/ponencia148_1.pdf Acceso: marzo 2012.

2.3. Situación actual de la Seguridad de la Información en Latinoamérica

A continuación presentamos los resultados de la III Encuesta Latinoamericana de Seguridad de la Información de la Asociación Colombiana de Ingenieros de Sistemas ACIS, 2011 [H], a través de un extracto de las preguntas que a nuestro criterio reflejan de manera más explícita las tendencias latinoaméricanas en cuanto a seguridad de la información. Dentro del grupo de paises participantes se encuentran: México, Argentina, Paraguay, Uruguay, Chile, Colombia, Perú, Brasil y algunas otras naciones de centroamérica. El nivel de participación oscila entre 300 y 400 profesionales en toda latinoamerica.

2.3.1. Resultados Encuesta de la Seguridad de la Información en Latinoamérica

Nivel de Participación en la encuesta

El mayor nivel de participación en la encuesta durante el 2009, 2010 y 2011 presenta Colombia:

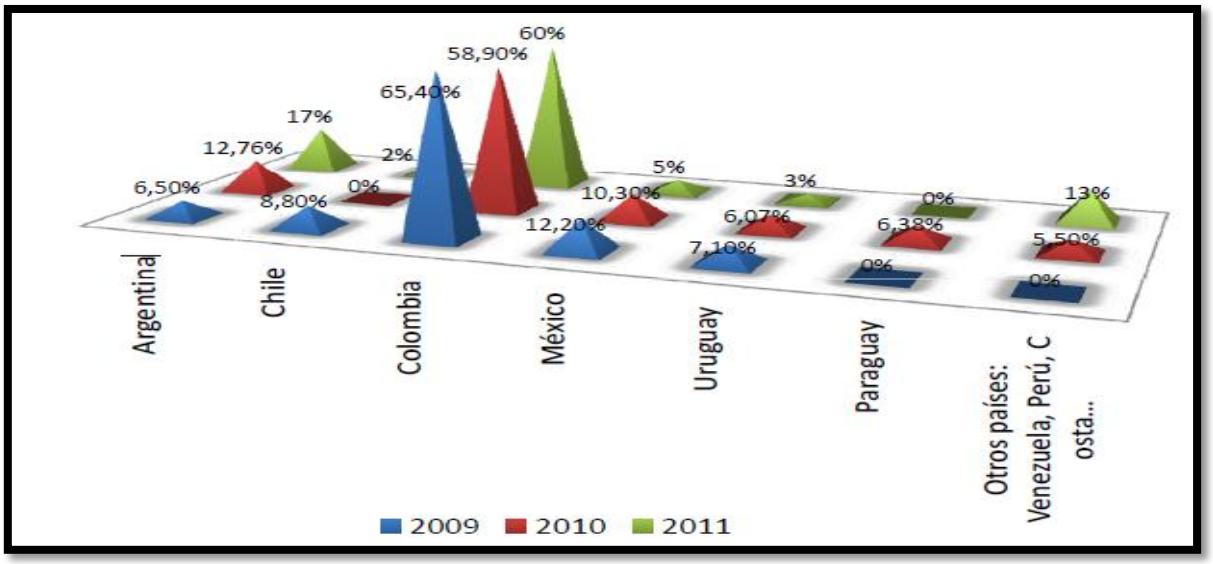


Figura 2-04 Nivel de Participación en Seguridad de la Información - por País[H]

[H] Jeimy J. Cano, ACIS, *XI Jornada de Seguridad Informática Seguridad de la Información: Una nueva década para avanzar, III Encuesta Latinoamericana de Seguridad de la Información ACIS 2011* , 2011.

Presupuestos

Si bien las exigencias de nuevos marcos regulatorios hacen que el tema de seguridad adquiera la relevancia requerida en las organizaciones, las desaceleraciones económicas mundiales afectan este tipo de inversiones. En los resultados, se observa que los presupuestos previstos para la seguridad han disminuido en el año 2011.

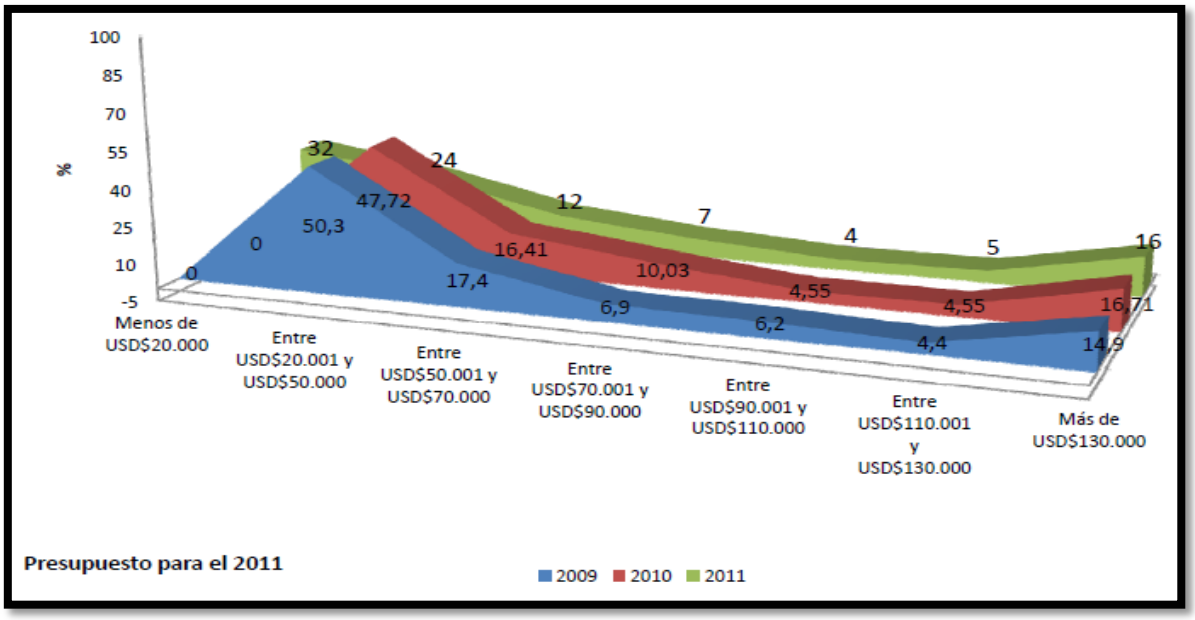


Figura 2-05 Presupuesto en Seguridad de la Información[H]

Incidentes de Seguridad

Se observa que en relación a los años 2009 y 2010, la ocurrencia de incidentes ha disminuido considerablemente en el 2011. Los virus e instalación de software no autorizado se mantienen, aunque en menor grado como los incidentes más frecuentes. Además se observa que los incidentes por caballos de troya y pérdida de información han disminuido, mientras que los ataques por Phishing han aumentado en relación al 2010.

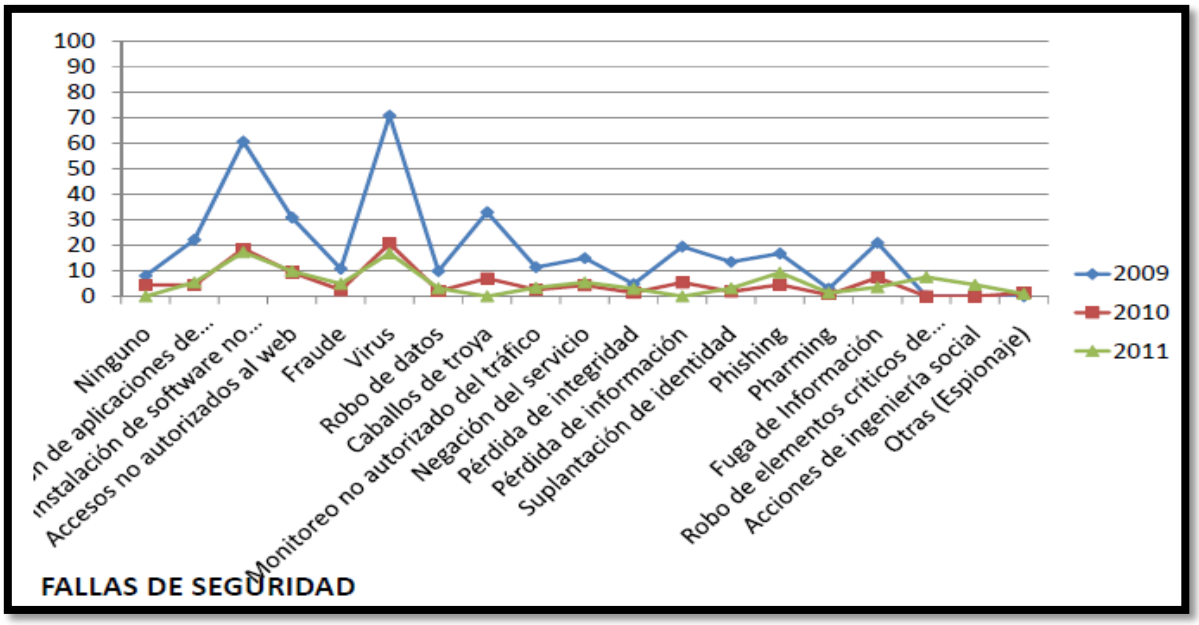


Figura 2-06 Incidentes de Seguridad[H]

Notificación de Incidentes de Seguridad

Se observa que desde el 2011, los incidentes se comienzan a reportar desde el nivel directivo de las organizaciones, lo que confirma que los puestos directivos están concientizando acerca de la importancia de la seguridad de la información.

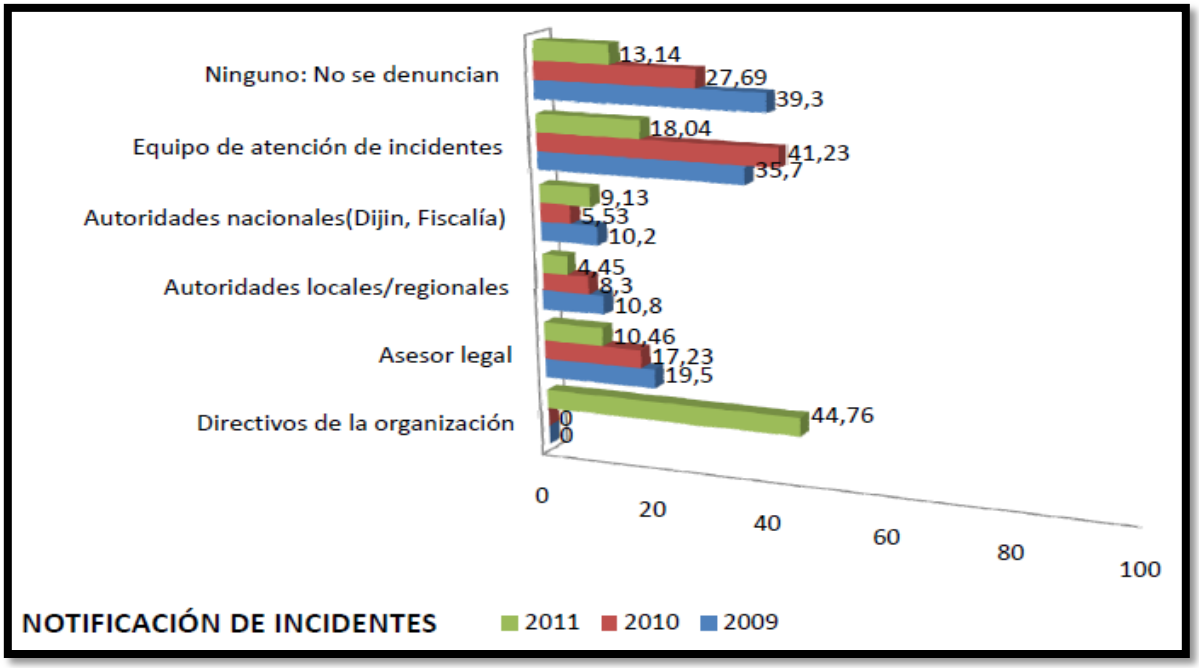


Figura 2-07 Notificación de Incidentes de Seguridad[H]

Políticas de Seguridad de la Información

Se observa que la conciencia para implementar políticas de seguridad se mantiene en el año 2011, sin embargo no ha aumentado porque las empresas ya la han adquirido disponen o se encuentra en desarrollo.

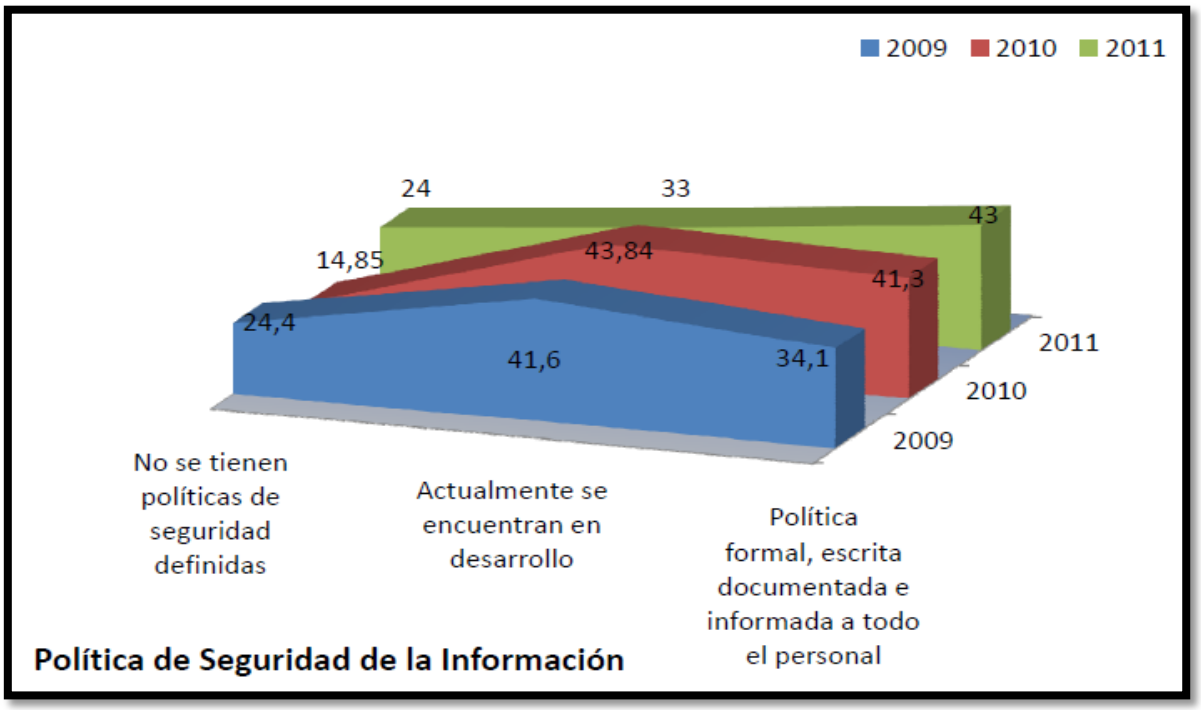


Figura 2-08 Políticas de Seguridad de la Información[H]

Obstáculos para implementar la seguridad

Entre los obstáculos para la implementación de seguridad en las empresas para el año 2011 se tienen entre los más altos: el poco entendimiento del tema, la falta de colaboración de las áreas y la falta de apoyo de los niveles directivos. Estas cifras hablan del limitado entendimiento de la seguridad de la información en el contexto de negocio, de la poca creatividad de los profesionales de la seguridad para vender la distinción de la seguridad y la necesidad de desarrollar un lenguaje que permita la integración entre el proceso y la protección de la información.

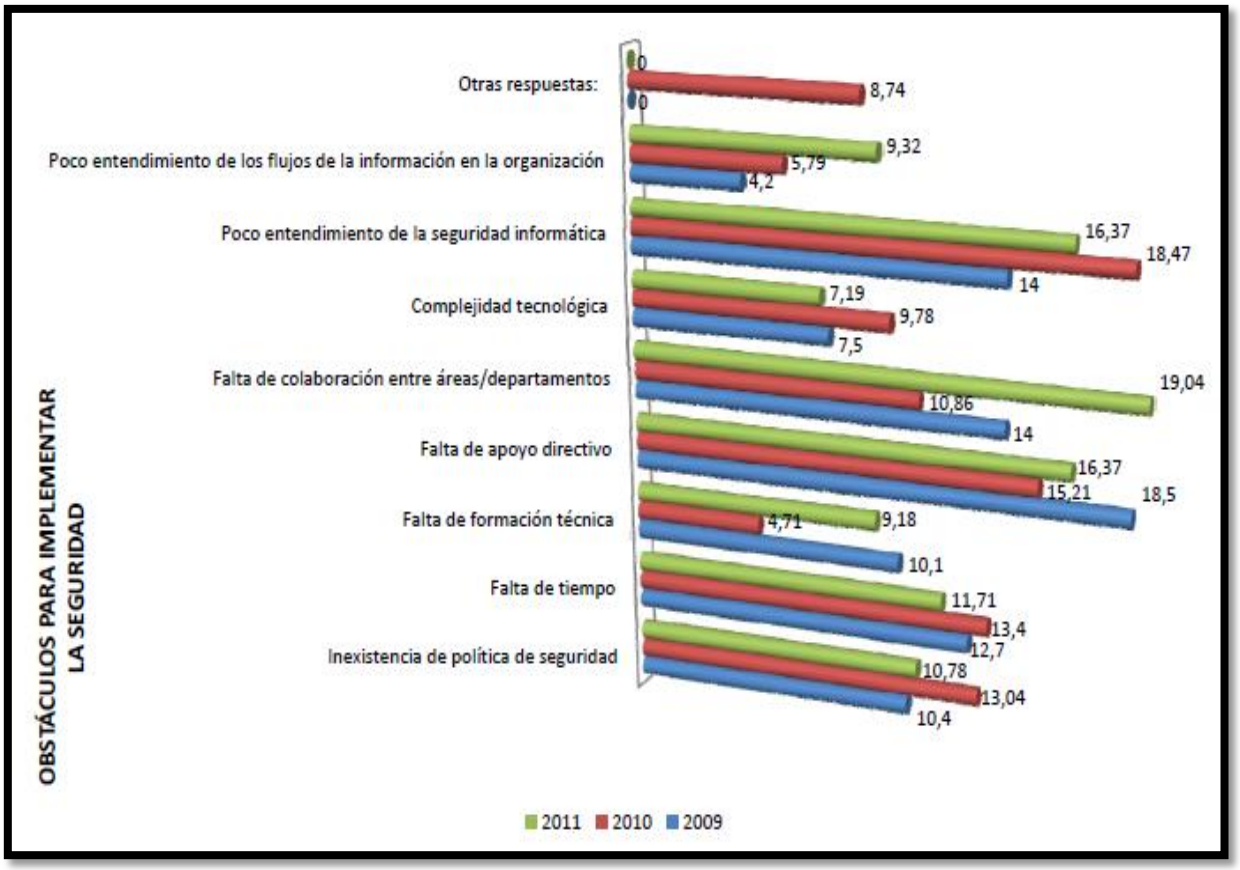


Figura 2-09 Obstáculos para Implementar la Seguridad de la Información[H]

Cada año son millones las organizaciones que padecen amenazas. Las empresas que logran superar estos traumas son las previsoras, las que están preparadas para enfrentarse a lo peor, las que estiman los posibles daños que pueden sufrir y ponen en marcha las medidas necesarias para protegerse.[E]

2.4. Estándares de Seguridad de la Información

Las constantes amenazas a la seguridad de la información en las empresas crean la necesidad de implementar contramedidas para reducir los riesgos generados a causa de las vulnerabilidades existentes. Dada la importancia que tiene la seguridad de la información en las organizaciones, se han creado estándares para la implementación de las mejores prácticas de seguridad alrededor del mundo.

[E] Inteco – Deloitte, *Guía para PYMES, Cómo Implantar un Plan de Continuidad del Negocio*, 2010, página 12.

Según el estudio "Principales Estándares para la Seguridad de la Información IT" de Flor Nancy Díaz Piraquive[I], las siguientes razones han puesto en evidencia la necesidad de que las empresas cuenten con un estándar de seguridad:

- Establecer un reglamento de prácticas favorables para la gestión de la seguridad.
- Establecer las especificaciones para la adopción de un Sistema de Gestión de la Seguridad de la Información.
- Establecer un conjunto de normas que se apliquen en cualquier entorno y sector, y que utilicen tecnologías de la información para lograr los objetivos propuestos.
- Mejorar los niveles de competitividad, optimizando la seguridad y el funcionamiento de la empresa.
- Promover servicios para que la empresa se incorpore más fácil y eficientemente a la sociedad de la información.

Estas razones hacen indispensable contar con un Sistema de Gestión de la Seguridad de la Información SGSI para garantizar la seguridad de la información en la empresa que quiera ser competitiva en el mercado. Es importante generar un estándar sobre el cual la empresa pueda converger y comunicarse en forma globalizada.

La presente información se basa en el estudio mencionado de Flor Nancy Díaz Piraquive[I] en el cual se determinarán las características básicas de los estándares más relevantes, por su nivel de aceptación.

2.4.1. Estándar RFC2196

Es estándar RFC2196 Site Security Handbook se estructuró y compendió en el año 1997.

Este estándar es un esfuerzo por dar cuerpo a las iniciativas de seguridad en el entorno a los sistemas de información y se enfoca en generar un marco conceptual para definir de manera integrada un esquema de seguridad basado en políticas a todo nivel en los temas referentes al manejo de la información, entre los que se destacan hardware, software, datos, personal involucrado, documentación y consumibles.

[I] Flor Nancy Díaz Piraquive, "Principales estándares para la seguridad de la información IT Alcances y consideraciones esenciales de los estándares ISO-IEC BS7799-IT, RFC2196, IT BASELINE, SSE-CMM y, ISO 27001", *Revista EOS No. 2,* Colombia, enero – abril 2008, pág 80.

De acuerdo con este enfoque es importante señalar que todo parte de la conceptualización del análisis de riesgo, donde es vital identificar dos aspectos: assets (activos - hardware, software, red, información y personal) y riesgos (vulnerabilidades, debilidades). Los activos y los riesgos van de la mano a la hora de implantar las políticas de seguridad, ya que cada uno de los activos presentará sus propios riesgos, con lo cual estructurar un plan de seguridad tendrá como base el estudio de las vulnerabilidades para cada uno de ellos.

La RFC2196 parte de esta premisa para que los responsables de las políticas de seguridad, en lo que respecta a las tecnologías de información, tengan claro el alcance de la implantación, con la estructura lógica que se presentará a continuación:

- Definición de objetivo: Se enfoca en la identificación del plan de seguridad, partiendo de un esquema en el cual, identificadas las amenazas, se procede a asegurar el sistema. La respuesta a incidentes será la parte fundamental, y separar los servicios a los cuales pueden o deben acceder los usuarios e identificar las necesidades para cada uno de ellos ayudarán a la estructuración de los objetivos del sistema.
- Configuración de servicios y red: Investigaciones, procesos, documentos, listas de precios y demás informaciones relacionadas con la operación de la empresa hacen que éstas se diferencien en los mercados actuales, cada vez más competitivos.
- Firewalls: Es común encontrar falencias en lo que respecta a procesos de seguridad informática (seguridad lógica) en las organizaciones. La seguridad no puede finalmente circunscribirse a los elementos hardware dispuestos en la red para permitir o no el acceso a los recursos e información de las organizaciones.
- Procedimientos y seguridad en servicios: Equipos, personal, políticas, procedimientos y procesos forman en sí un sistema integrado de seguridad. El acceso de la información debe tener un esquema donde se puedan seguir ciertos procedimientos que han de estructurarse tomando como base las necesidades de la organización.

Por otro lado, la RFC2196 hace hincapié en los siguientes procesos al momento de estructurar los procedimientos, teniendo como base los elementos que componen el sistema de información:

- Autenticación: Determinar si el solicitante del servicio o información es, de hecho, quien tiene derecho a usarla.
- Autorización: Dar permiso al solicitante de realizar o no acciones dentro de un sistema.

- Integridad y confidencialidad: Asegurar que la información no sea alterada y que va a mantenerse en un entorno controlado para no difundir su contenido, en este orden.
- Acceso: Establecer los mecanismos por los cuales los solicitantes van a acceder a los recursos de información de la organización, ya sea desde el interior o desde el exterior.
- Auditoría: Los procesos anteriores deben cobijarse mediante un procedimiento de auditoría. Saber quién, en qué momento y cuál fue la labor realizada sobre la información o sobre los sistemas, deberá registrarse en algún sitio para tener control sobre los incidentes.
- Manejo de incidentes: Evitar los problemas de seguridad de la información a través de la implantación de un sistema que incluya todos los activos involucrados en la organización. En caso de falla, el esquema deberá responder de la mejor manera frente a los incidentes que afecten la información, minimizando su impacto. Teniendo como base esta premisa, el manejo de incidentes se debe preparar y planear para cumplir este objetivo.

Además, el RFC-2196 establece una serie de componentes incluidos en las políticas de seguridad. Éstos son:

- Guías de compras de tecnología de la información: Especifica funciones de seguridad requeridas o preferidas.
- Política de privacidad: Determina las expectativas razonables de privacidad sobre temas relacionados con monitoreo de correos electrónicos, acceso a archivos y registro de teclados. Podría incluir también políticas acerca de registro, escucha y control de llamadas telefónicas, control de accesos a sitios web, uso de herramientas de mensajería instantánea.
- Política de acceso: Define derechos o privilegios de acceso a activos o recursos de información protegidos. Especifica comportamientos aceptables para usuarios, empleados soporte y directivos.

  Debe incluir reglas respecto a las conexiones y accesos externos, así como reglas acerca de la comunicación de datos, conexiones de dispositivos a las redes e inclusión de nuevas aplicaciones informáticas en los sistemas existentes.
- Política de responsabilidad: Define las responsabilidades de usuarios, personal de mantenimiento y directivos. Debe especificar la capacidad de realizar auditorías y sus características, y proveer las guías para el registro y manejo de incidentes de seguridad.

- Política de autenticación: Debe establecer los mecanismos de "confianza" mediante el uso de una política de contraseñas apropiadas. Debe considerar, si aplica, políticas de autenticación local y de acceso remoto.
- Declaración de disponibilidad: Determina las expectativas de disponibilidad de los recursos de los sistemas e información. Con base en la disponibilidad necesaria, podrán establecerse mecanismos de redundancia y procedimientos de recuperación.
- Política de mantenimiento de los sistemas relacionados con la tecnología de la información: Describe cómo deberá hacerse el mantenimiento realizado tanto por personal interno como externo a la organización. Debe establecerse si se admite o no algún tipo de mantenimiento remoto (por ejemplo, por internet o por módem), y las reglas que aplican, así como los mecanismos internos de control.
- Política de informes de incidentes o violaciones de seguridad: Establece qué tipo de incidentes o violaciones de seguridad deben reportarse y a quién reportar. Para no generar un ambiente "amenazante", puede considerarse la inclusión de reportes anónimos, lo que seguramente redundará en una mayor probabilidad de que los incidentes sean efectivamente reportados.
- Información de apoyo: Proveer a los usuarios, empleados y directivos con información de contacto y de referencia para usarla ante incidentes de seguridad. En todos los casos, los aspectos legales deben tomarse en cuenta.

2.4.2. Estándar IT Baseline Protection Manual

El IT Baseline Protection Manual presenta un conjunto de recomendaciones de seguridad, establecidas por la Agencia Federal Alemana para la Seguridad en Tecnología de la Información. Este estándar plantea en forma detallada aspectos de seguridad en ámbitos relacionados con aspectos generales (organizacionales, gestión humana, criptografía, manejo de virus, entre otros); infraestructura, (edificaciones, redes wifi); sistemas (Windows, Novell, Unix); redes (cortafuegos, módems), y aplicaciones (correo electrónico, manejo de la web, bases de datos, aplicativos.

Los objetivos del estándar son asistir en forma rápida con soluciones a problemas comunes en seguridad e identificar los riesgos de seguridad de Tecnologías de Información - TI.

De la misma manera, define su alcance aduciendo que el IT Protection Manual contiene estándares de protección de seguridad de tecnologías de información e implanta conceptos de seguridad de IT, simplificando y economizando los recursos requeridos.

El análisis de la estructura de IT provee los medios para la realización de un estudio preliminar, apuntando a la recolección de información que se necesitará después, para preparar el concepto del IT baseline protection security. Esto se divide en las siguientes subtareas: preparar el plan de red, reducir la complejidad identificando recursos similares, recolectar información sobre los sistemas de IT, y captar información sobre las aplicaciones de IT y relacionarla con ésta.

- Procesos de seguridad IT: La función primaria de la administración de seguridad IT es preparar los conceptos de seguridad, los cuales son indispensables para la implantación de los procesos.
- Evaluación de requerimientos de protección: Para evaluar modelos de protección de la estructura de IT se requieren cuatro pasos por separado. El primero de todos es definir las categorías de requerimientos de protección.
- Modelo de protección IT Baseline: Se enfoca de acuerdo con un orden descendente, así: activos de IT, análisis de la estructura de IT, evaluación de los requerimientos de protección y modelamiento. De este último se desprenden dos actividades: ejecutar el plan sobre los activos IT en uso y desarrollar el plan sobre los activos de IT planificados.
- Chequeo de seguridad básica: El módulo de protección de IT se utiliza como un plan de prueba para establecer, usando un objetivo frente a la actual comparación, cuál estándar para salvaguardar la seguridad ha sido efectivo y cuál no se ha implementado efectivamente.
- Análisis de seguridad suplementario: Un análisis de seguridad de IT suplementario se debe entregar para puntos sensibles de la organización. Se pueden emplear varios métodos, que incluyan análisis del riesgo, pruebas de penetración y análisis diferencial de seguridad.
- Implementación de modelo de protección de seguridad IT: Se destacan los siguientes pasos: examinar los resultados de la investigación, consolidar los salvaguardas, preparar un estimado de costos y esfuerzos requeridos, determinar la secuencia de implementación, asignar responsabilidades e implantar medidas de acompañamiento.

2.4.3. Estándar SSE-CMM

El Systems Security Engineering Capability Maturity Model - SSE-CMM es, más que un estándar, un modelo de referencia que no dicta normas estáticas en lo que concierne a la seguridad en los ambientes de información y tecnología (IT) que quiere enmarcar su radio de acción. Este modelo es un esfuerzo multilateral dirigido por la Universidad de Carnegie Mellon en Estados Unidos. Debido a que su alcance no restringe a una práctica especifica en la implantación de seguridad de la información, se manejan conceptos generales para entender el modelo. Éste se basa en la definición de conceptos como organización, proyecto, sistema, producto de trabajo, cliente, proceso, institucionalización, gerencia de proceso y Modelo de Capacidad de Madurez - CMM. Este último concepto sirve para describir cómo, a través del proceso de planeación, implantación y mejoras, el modelo se ajusta a cada situación particular; es tratar de identificar qué tan "maduro" se encuentra el esquema planteado para la seguridad de información en la organización.

Se fundamenta en la presentación de una serie de actividades para desarrollar productos de software confiables y alcanzar un ciclo de vida para sistemas seguros.

De todos los modelos presentados, éste es el que mayor relación y adecuación tiene respecto al desarrollo de productos de software seguros. SSE-CMM divide la ingeniería de seguridad en tres áreas básicas: riesgo, ingeniería y aseguramiento.

- Riesgo: busca identificar y priorizar los peligros asociados al desarrollo de productos o sistemas.
- Ingeniería: trabaja con otras disciplinas para implantar soluciones sobre los peligros identificados. En este caso, se relaciona con la ingeniería de software.
- Aseguramiento: tiene como objetivo certificar que las soluciones implementadas sean confiables.

El modelo se estructura en dos dimensiones:

- Dominios: conjunto de prácticas básicas que definen la ingeniería de seguridad.
- Capacidades: se refiere a las prácticas genéricas que determinan la administración del proceso e institucionalizan la capacidad.

La propuesta se hace considerando que la ingeniería de seguridad no es una actividad que pueda desarrollarse de manera aislada de otras especialidades de la ingeniería, en especial de la ingeniería de sistemas y de software.

El modelo se enfoca en la ingeniería de seguridad como marco para desarrollar un esquema confiable alrededor de la temática de aseguramiento en entornos de información y tecnología. Por ello es importante mencionar el ciclo de vida de ingeniería de seguridad, de acuerdo con el modelo concepto, desarrollo, producción, utilización, soporte y retiro son etapas inherentes a las actividades que soportan el modelo mencionado. Como tal, la arquitectura del sistema se basa en tres macroprocesos: evaluación de riesgo, ingeniería de seguridad y aseguramiento. Con ello se da forma a una matriz que pretende realizar un diagnóstico y establecer qué grado de madurez tiene la estrategia de seguridad en una organización. Este último concepto sirve para describir cómo, a través del proceso de planeación, implantación y mejoras, el modelo se ajusta a cada situación particular; es tratar de identificar qué tan "maduro" se encuentra el esquema planteado para la seguridad de información en la organización.

2.4.4. Estándar ISO/IEC 17799[B]

A inicios de la década de los 90, el Departamento de Comercio e Industria del Reino Unido inicia el desarrollo de una Norma Británica - BS, para proteger y regular la gestión de seguridad en las empresas y los gobiernos. La primera norma (BS 7799:95) fue oficialmente aprobada en 1995 y nace como un código de mejores prácticas para la gestión de seguridad de la información. Luego de esta normalización, le han seguido las siguientes:

- 1998: Publicación de la primera edición de la norma BS 7799-2, la cual contiene especificaciones para la gestión de la seguridad de la información y se lanzan requerimientos certificables por primera vez.
- 1999: Publicación de la segunda edición la norma BS 7799-2, en la que se añade "e-commence" al alcance de la misma. La Organización Internacional de Estándares - ISO comienza a interesarse por los trabajos publicados por el Instituto inglés.
- 2000: Tras una revisión de ambas partes de la norma BS 7799-2, se aprueba la norma ISO 17799[B] Parte 1, que es el código de práctica para los requisitos de gestión de seguridad de la información (no certificable). Esta norma está formada por un conjunto completo de controles que conforman las buenas prácticas de seguridad de la información, y que pueden ser aplicadas por toda organización con independencia de su tamaño.

- 2002: Revisión de la parte 2 de la BS 7799-2:2002 (certificable), con el fin de armonizarla con otras normas de gestión tales como la ISO 9001:2000 y la ISO 14001:1996, así como con los principios de la Organización para la Cooperación y el Desarrollo Económicos - OCDE.
- 2005: Publicación de la norma ISO 27001[J], norma certificable y que reemplaza a la BS 7799-2. Este reemplazo se debió principalmente por:
  - Ascenso al estado de internacional
  - Se esperó que más empresas lo adopten
  - Mejoras y aclaraciones realizadas por la ISO
  - Alineación en las definiciones con otros estándares ISO (por ejemplo, ISO/IEC 1335-1:2004 e ISO/IEC TR 18044:2004). IEC es la Comisión Internacional de Electrotécnica.

Este código apunta a crear un marco de buenas prácticas para el manejo de seguridad de la información y su interoperatividad con los sistemas basado en el esquema Plan Do Check Act - PDCA:

- Planear (plan) en este entorno significa definir políticas de seguridad y su alcance. Las políticas no podrán ser efectivas si no se articulan en torno a riesgos que deben evaluarse en la organización.

  Identificar y evaluar opciones para tratar esos riesgos y seleccionar para cada riesgo la mejor opción de tratamiento son aspectos importantes durante la fase de planeación sugerida por el estándar.
- Ya en la parte de implementación (DO) se deben formular los planes de tratamiento de riesgos y su implantación. De igual manera, se ha de implementar el esquema de procedimiento de detección y respuesta a los incidentes, teniendo previamente un personal capacitado.
- Verificar y auditar (Check- Audit). Monitorear, revisar, probar y auditar cierran el ciclo de estructuración de políticas contenidas dentro del manejo de incidencias de seguridad de información.
- Estructura del estándar. Este estándar se enfoca en la identificación de riesgo y su tratamiento para asegurar la confidencialidad, disponibilidad e integridad de la información.

2.4.5. Estándar ISO/IEC 27001[J]

Este es el estándar oficial. Su título completo en realidad es BS 7799-2:2005 (ISO/IEC 27001:2005[J]). La ISO y la IEC son entidades que conforman un sistema especializado de estándares mundiales. Estas entidades se constituyen de organismos miembros y de organizaciones internacionales, gubernamentales y no gubernamentales relacionadas, que a través de sus comités técnicos especializados - JTC1 participan en el desarrollo de Normas Internacionales. Los borradores de las Normas Internacionales desarrolladas por los Comités Técnicos son enviados a los organismos de las diferentes naciones para su votación. Su publicación requiere la aprobación de al menos 75% de votos.[J]

ISO ha reservado la serie de la numeración 27000 para todas las normas relacionadas con sistemas de gestión de seguridad de información. Como se ha mencionado, en el 2005 incluyó la primera parte de la serie 27001, las demás son:

- ISO27000 (términos y definiciones),
- ISO27002 (objetivos de control y controles),
- ISO27003 (guía de implantación de un SGSI),
- ISO27004 (métricas y técnicas de medida de la efectividad de un SGSI),
- ISO27005 (guía para la gestión del riesgo de seguridad de la información) y
- ISO27006 (proceso de acreditación de entidades de certificación y el registro de SGSI).

El ISO/IEC 27001:2005[J] es el único estándar aceptado internacionalmente para la administración de la seguridad de la información y aplica a todo tipo de organizaciones, tanto por su tamaño como por su actividad. El alcance se concibe hasta proveer un modelo para el establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora del SGSI. Se proporcionará más información con respecto al presente estándar en el capítulo III - ISO/IEC 27001:2005[J].

[J] Estándar Internacional ISO/IEC 27001, *Tecnología de la Información – Técnicas de Seguridad – Sistemas de Gestión de Seguridad de la Información – Requerimientos*, Colombia, octubre 2005.

2.5. Evaluación de estándares de seguridad de la información

En la siguiente matriz[I] se comparan los aspectos más relevantes de los estándares de seguridad presentados, con la finalidad de obtener una mejor idea del estándar más aceptado internacionalmente y por ende más apropiado para aplicar en una empresa Industrial de la Provincia de Pichincha en el Ecuador.

Matriz de Comparación de los Estándares Presentados					
	ISO-IEC BS7799-I	**RFC2196**	**IT BASE LINE**	**SSE-CMM**	**ISO-IEC 27001**[J]
Tipo	Estándar	Recomendación	Recomendación	Estándar	Estándar
Certificación	No	Local	No	Local	Internacional
Identifica activos informáticos y vulnerabilidad	Si	Si	Si	Si	Si
Identifica RRHH	Si	Si	Si	Si	Si
Se debe documentar	Si	Si	Si	Si	Si
Define claramente responsabilidades	Si	Si	Si	Si	Si
Establece, implementa, monitorea y mantiene SGSI	Si	Si	Si	Si	Si

Cuadro 2-01 Matriz de Comparación de los Estándares Presentados[I]

Complementariamente, presentamos a continuación una de las preguntas de la III Encuesta Latinoamericana de Seguridad de la Información ACIS 2011[H], la cual evidencia que entre las mejores prácticas mayormente aceptadas a nivel de Latinoamérica es el estándar ISO/IEC 27001:2005[J].

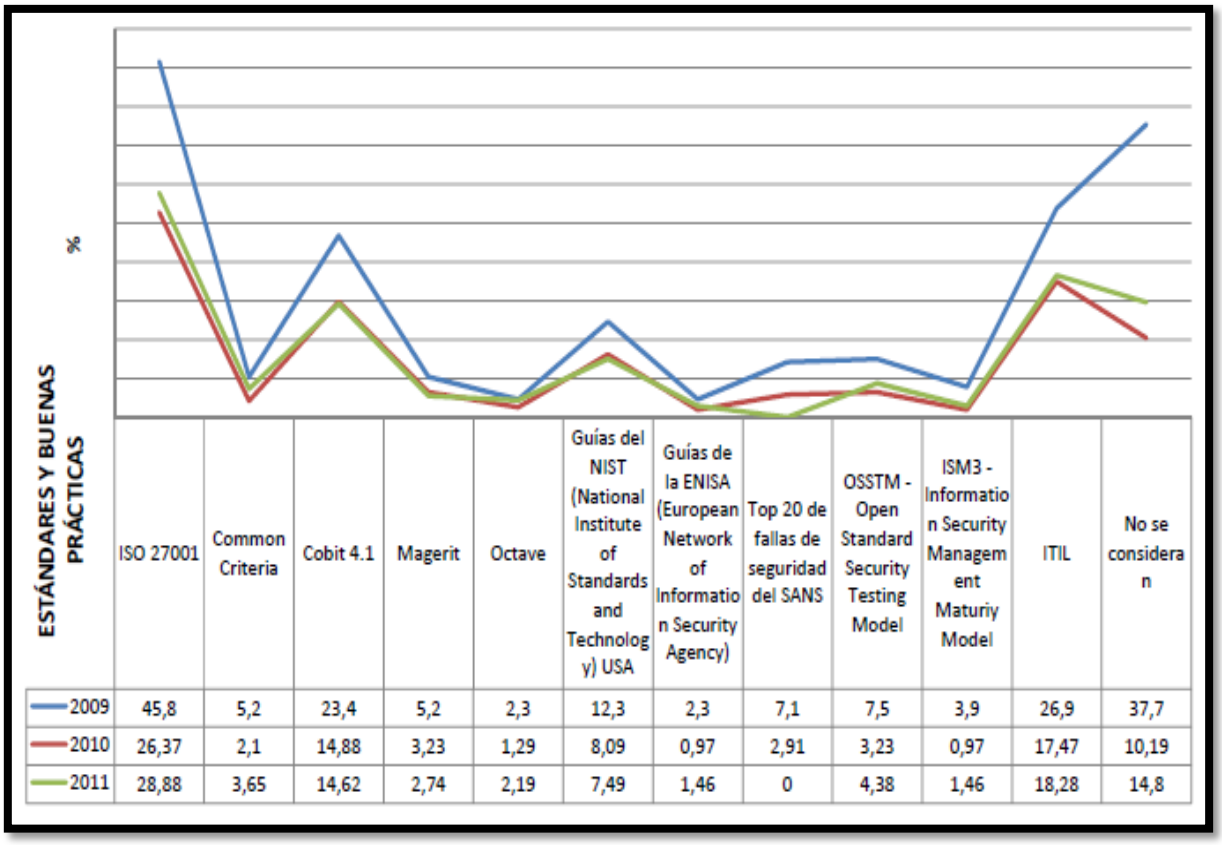


Figura 2-10 Estándares y Buenas Prácticas de la Seguridad de la Información[G]

Como conclusión, se observa la importancia del estándar ISO/IEC 27001[J] al ser reconocidos e impulsados mundialmente, incluyendo a Latinoamérica *(para mayor detalle, ver Anexo A "Síntesis del Estándar ISO/IEC 27001:2005" adjunto este documento de Tesis).*

Además, las más grandes empresas y gobiernos ya están certificándose en ella; dándose el caso incluso de países como Estado Unidos, que contando con sus propias normativas (la serie 800 del Instituto Nacional de Estándares y Tecnología - NIST), muchas de sus empresas y de sus instituciones públicas se están certificando en la norma, lo que da cuenta de su importancia y amplio respaldo, razón por la cual se plantea a esta norma en el tema del presente proyecto.

CAPÍTULO III: ESTÁNDAR ISO/IEC 27001:2005

El objetivo de este capítulo es conocer más detalladamente al estándar de Seguridad de la Información ISO/IEC 27001:2005[J], sobre el cual en el capítulo anterior se concluyó es el de mayor aceptación a nivel mundial por lo que es importante obtener más información y familiarizarnos con los conceptos y generalidades de la misma. Así tendríamos las bases para realizar el análisis costo beneficio en la empresa seleccionada.

3.1. Introducción al estándar ISO/IEC 27001:2005[J]

La ISO/IEC 27001:2005[J] define los requisitos exigibles para un Sistema de Gestión de la Seguridad de la Información - SGSI certificable y provee un proceso de gestión para su evaluación, implementación y mantenimiento mediante un conjunto de controles, en integración con las mejores prácticas en seguridad de la información aplicable a todos los sectores. Un SGSI certificado es el medio para que la empresa tenga niveles altos en la seguridad información, desarrolle y mejore el rendimiento del sistema y pueda competir con otras empresas en cualquier ámbito internacional o local.

Un SGSI es la mejor manera de supervisar, controlar y monitorear periódicamente el trabajo de una empresa en materia de seguridad de la información a través del establecimiento de políticas, procedimientos y controles que protegen los activos de información de la empresa independientemente del medio en que se encuentren (correo electrónico, informes, escritos relevantes, páginas web, imágenes, documentos, hojas de cálculo, faxes, presentaciones, contratos, registros, sistemas), resultando en la posible disminución significativa del impacto de los riesgos en la seguridad, sin la necesidad de realizar grandes inversiones.

En definitiva, con un SGSI la empresa conoce, asume, gestiona y minimiza los riesgos a los que está sometida su información; de manera sistemática, definida, estructurada, documentada, continua, repetible, eficiente y adaptada a los cambios que se produzcan en la empresa, los riesgos, entorno y tecnología. Además de ser conocida por todos en la empresa, revisada y mejorada constantemente.

Los objetivos principales de la ISO/IEC 27001:2005[J] son el de incorporar la seguridad dentro de la cultura y marco de gestión de la empresa y garantizar la confidencialidad, disponibilidad, e integridad de su información para que pueda cumplir con sus objetivos de negocio, así como sus requisitos contractuales y legales [10].

Según una encuesta llevada a cabo por el grupo empresarial dedicado al apoyo en la adopción de las mejores prácticas gerenciales, reducción de riesgos empresariales y aceptación de estándares internacionales, BSI-DISC en cooperación con Admiral Plc., las principales razones para buscar una certificación de SGSI son:

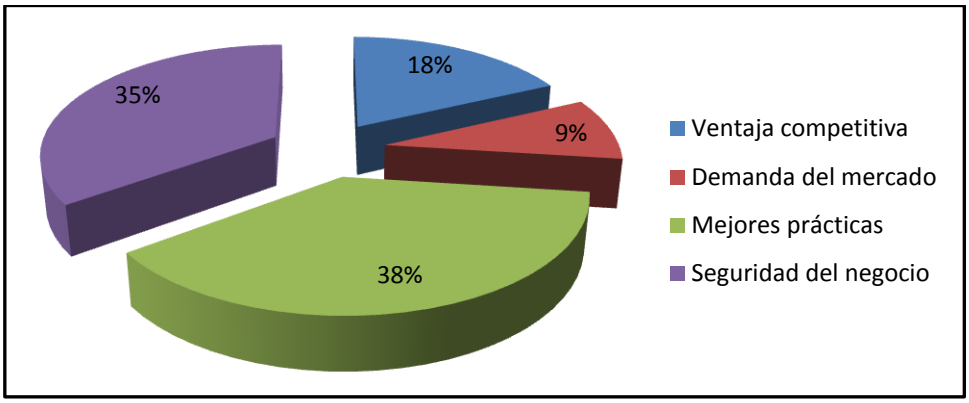


Figura 3-01 Razones para buscar una certificación SGSI[18]

La ISO/IEC 27001:2005[J] es un elemento de gestión que se irá generalizando en las empresas, distinguiéndose aquellas que se anticipen en su implementación.

"…se puede prever, que la certificación ISO-27001, será casi una obligación de cualquier empresa que desee competir en el mercado en el corto plazo…"[K]

Según el Instituto Internacional de Certificados SGSI[11] , actualizado a enero 2012 (versión 212), en la actualidad existen 7,686 empresas en 86 países que han reconocido la importancia y los beneficios de esta norma.

[10] ProactivaNet, *ISO27001…¿Por dónde empezamos?,* Internet. http://www.proactivanet.com/UserFiles/File/ProactivaNET%20-%20ISO%2027001.pdf Acceso, marzo 2012

[K] Alejandro Corletti Estrada, *Análisis de ISO-27001:2005*, Madrid, abril de 2006, pág 1.

[11] International Register of ISMS Certificates, versión 212, enero 2012, Internet. http://www.iso27001certificates.com/ Acceso, marzo 2012

A continuación se presenta la lista de países que han certificado a sus SGSI a través de la ISO/IEC 27001:2005[J], encabezando Japón con 4,004 certificaciones, Reino Unido con 536, India con 527 y China con 507. En este registro, Ecuador cuenta con una sola certificación (Telconet S.A.), sin embargo en febrero 2012, la empresa Telefónica Movistar Ecuador obtuvo una certificación, llegando a 2 certificaciones 27001 en el país.

Países con número de certificaciones ISO/IEC 27001[J]					
País	**#**	**País**	**#**	**País**	**#**
Japan	4004	Croatia	21	Gibraltar	3
UK	536	Slovenia	20	Macau	3
India	527	Bulgaria	18	Qatar	3
China	507	Iran	18	Albania	2
Taiwan	456	Philippines	15	Argentina	2
Germany	202	Pakistan	14	Bosnia Herzegovina	2
Korea	106	Saudi Arabia	14	Cyprus	2
Czech Republic	110	Vietnam	14	Isle of Man	2
USA	104	Iceland	13	Kazakhstan	2
Italy	81	Indonesia	13	Luxembourg	2
Spain	75	Colombia	11	Macedonia	2
Hungary	70	Kuwait	11	Malta	2
Poland	62	Norway	10	Ukraine	2
Malaysia	58	Portugal	10	Mauritius	2
Thailand	48	Sweden	10	Armenia	1
Austria	44	Canada	9	Bangladesh	1
Ireland	44	Russian Federation	9	Belarus	1
Romania	35	Switzerland	9	Denmark	1
Hong Kong	32	Bahrain	8	Ecuador	1
Greece	31	Egypt	5	Jersey	1
Australia	29	Oman	5	Kyrgyzstan	1
Singapore	29	Peru	5	Lebanon	1
Mexico	27	Sri Lanka	5	Moldova	1
France	26	Dominican Republic	4	New Zealand	1
Slovakia	26	Lithuania	4	Sudan	1
Turkey	26	Morocco	4	Uruguay	1
Brazil	24	South Africa	4	Yemen	1
UAE	20	Belgium	3		
Netherlands	22	Chile	3	**Total**	**7686**

Cuadro 3-01 Países con número de certificaciones SGSI[11]

[18] Inger Nordin, "Accreditation and certification ISMS EA Guidelines for ISMS Certification Process", 2003, Internet, http://www.docstoc.com/docs/55751922/Accreditation-and-certification-ISMS-EA-Guidelines-for-ISMS. Acceso: mayo 2012

Cabe mencionar que las empresas a nivel mundial que certificaron a sus SGSI con la norma británica BS 7799 (revisada en el segundo capítulo, punto 2.4.4) pasaron a estar certificadas en ISO/IEC 27001[J], según el comunicado para la transición realizado por UKAS en Junio del año 2006 en donde comunica a las compañías certificadas en la norma británica BS 7799-2:2002 hacer efectiva la transición hasta julio del año 2007.

3.2. Contenido del estándar ISO/IEC 27001:2005[J]

Este estándar no está orientado hacia temas técnicos o de infraestructura, tampoco está impulsado por la adquisición de productos o tecnología, sino a aspectos netamente estratégicos y organizativos, proporcionando a la gerencia una visión global sobre el estado de sus sistemas de información, las medidas de seguridad que se están aplicando y los resultados que se están obteniendo de esta aplicación, para la toma de decisiones.

De ahí se dice que la norma ISO/IEC 27001:2005[J] define como "organizar la seguridad de la información" en las empresas, por ello dispone de una secuencia de acciones con tendencias hacia el establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora de un SGSI documentado, teniendo en cuenta las problemáticas y riesgos de seguridad empresariales. En general, los detalles que cubren la ISO/IEC 27001:2005[J] se podrían agrupar en 3 grandes líneas:

- SGSI,
- Gestión de riesgos y controles;
- De manera específica, 11 dominios, ilustrados a continuación:

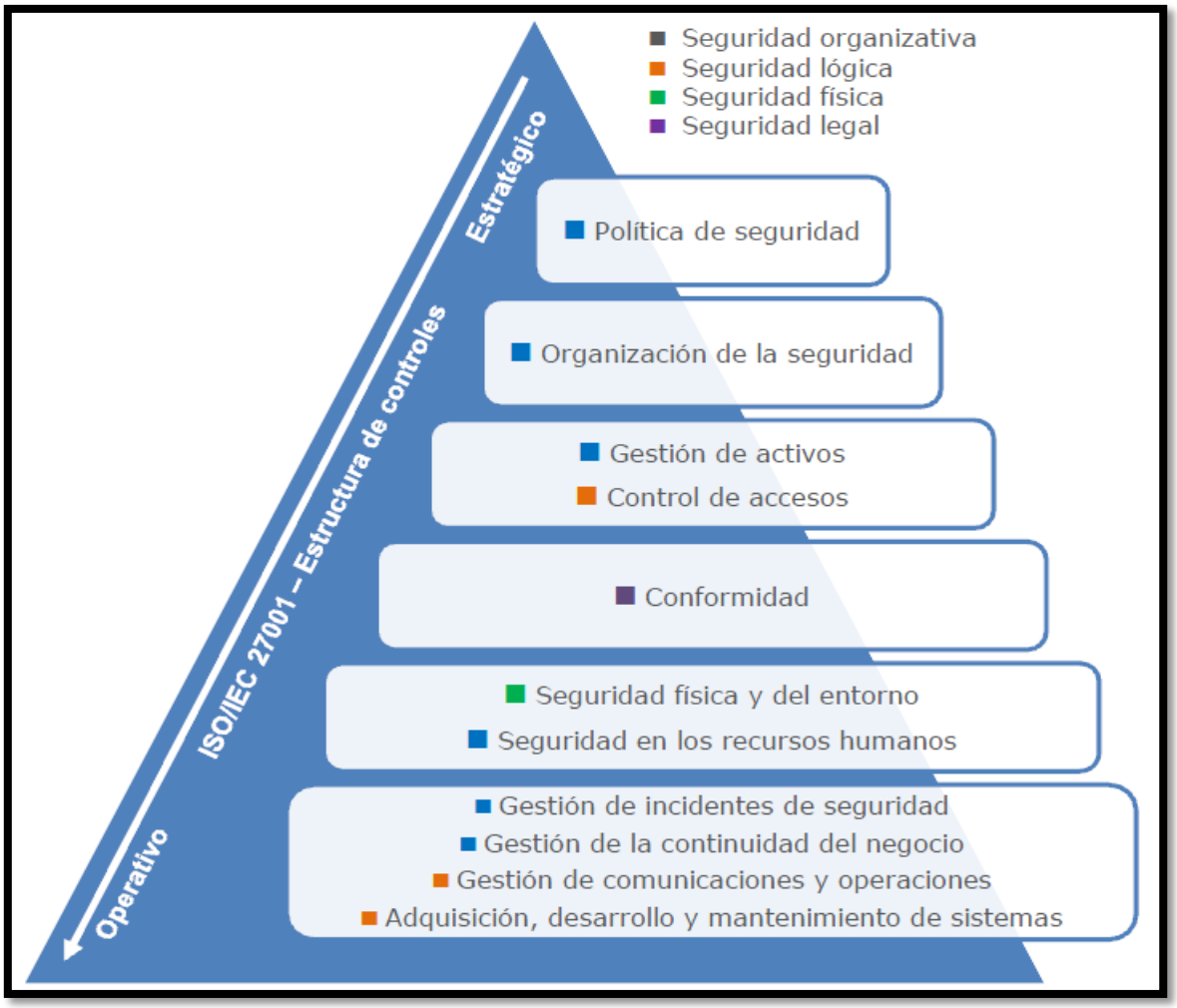


Figura 3-02 Dominios del estándar ISO/IEC 27001[10]

De estos 11 dominios se derivan 39 objetivos de control (resultados que se esperan alcanzar mediante la implementación de controles) y 133 controles (prácticas, procedimientos o mecanismos que reducen el nivel de riesgo de la información empresarial). La estructura del estándar ISO/IEC 27001:2005 es la siguiente: [J]

Para mayor detalle, ver Anexo A "Síntesis del Estándar ISO/IEC 27001:2005" adjunto este documento de Tesis.

1. Alcance
    1.1. Generalidades
    1.2. Aplicación
2. Referencias normativas
3. Términos y definiciones
4. Elementos del Sistema de Gestión de Seguridad de la Información
    4.1. Requisitos generales
    4.2. Establecimiento y gestión del SGSI
        4.2.1. Establecimiento del SGSI
        4.2.2. Implantación y operación del SGSI
        4.2.3. Seguimiento y revisión del SGSI
        4.2.4. Mantenimiento y mejora del SGSI
    4.3. Requisitos de la Documentación
        4.3.1. Generalidades
        4.3.2. Control de los documentos
        4.3.3. Control de los registros
5. Responsabilidad de la Dirección
    5.1. Compromiso de la Dirección
    5.2. Gestión de Recursos
        5.2.1. Provisión de recursos
        5.2.2. Formación, conocimiento y competencia
6. Auditorías internas del SGSI
7. Revisión del SGSI
    7.1. Generalidades
    7.2. Entradas o datos iniciales para la revisión
    7.3. Salidas o resultados de la revisión
8. Mejora continua del SGSI
    8.1. Mejora continua
    8.2. Acción correctiva
    8.3. Acción preventiva

- Anexo A: Anexo normativo que enumera en una tabla los objetivos de control y controles detallados en la norma ISO 27002:2005.
- Anexo B: Anexo informativo que relaciona los principios del buen gobierno de la OCDE - Organización para la Cooperación y el Desarrollo Económicos (en inglés, OECD - Organisation for Economic Co-operation and Development) con los apartados correspondientes en la ISO/IEC 27001:2005.
- Anexo C: Anexo informativo que señala la correspondencia de la ISO/IEC 27001:2005 con otras normas como ISO 9001 e ISO 14001 mediante una tabla.

3.3. Beneficios de la aplicación del estándar ISO/IEC 27001:2005[J]

Los beneficios más relevantes de certificarse y cumplir con la ISO/IEC 27001:2005 están:

- Es la única norma certificable y auditable con aceptación global.
- Mejora y formaliza a la gestión de la seguridad de la información en una empresa en base de procesos que forman un ciclo de vida metódico y controlado en lugar de la compra sistemática de productos y tecnologías, involucrando y comprometiendo a la alta gerencia como propietaria de esta responsabilidad.
- Partiendo de la evaluación de riesgos que imparte la norma hasta la implementación de controles, se facilita la continuidad de las operaciones de negocio tras incidentes de gravedad que atentan a la información de la empresa (errores, sabotajes o desastres).
- Establece objetivos de seguridad y calidad medibles para la evaluación de su éxito y ofrece un criterio de mejora continua de los mismos.
- La implementación de la norma permite una racionalización de recursos, lo que repercute en un ahorro de costes. Al permitir que la gerencia tome decisiones basadas en datos cuantitativos y no solo cualitativos, se puede administrar mejor el gasto en TI, por lo que las inversiones en tecnología se ajustan a las prioridades que se han impuesto a través del Análisis de Riesgos, evitando gastos innecesarios, inesperados y sobredimensionados.
- Cobertura de varios aspectos dentro de la empresa tanto a nivel estratégico como temas de tecnología de la información, capital humano e instalaciones.
- Proporciona un enfoque en las responsabilidades y aumento de la motivación y satisfacción del personal, provocando un cambio de cultura corporativa interna y externa, resultando en una mayor conciencia y compromiso sobre la importancia de la seguridad en todos los niveles de la empresa.
- Ofrece confianza para socios comerciales, accionistas y clientes al demostrar el compromiso de la empresa con la seguridad de la información frente a terceros (la certificación demuestra el principio de la ‘debida diligencia’), mejorando su imagen, credibilidad y diferenciación en el mercado.
- Permite el cumplimiento de reglamentaciones y requisitos legales vigentes en cada país (actualmente, la Asamblea Nacional del Ecuador está trabajando en el proyecto de Ley de Protección a la Intimidad y a los Datos Personales), por lo tanto la certificación garantiza este hecho y seguramente crea un marco legal que protegerá a la empresa en aspectos que seguramente no se habían tomado en cuenta anteriormente.

- Se pueden obtener posibles reducciones en las primas de seguros, vinculadas a disminuciones de accidentes en materia de seguridad de información.
- Combina recursos con otros sistemas de gestión (por ejemplo con el Sistema de Gestión de Calidad, ISO 9001, ISO 14001, Servicios de Consultoría de Salud Ocupacional y Seguridad - OHSAS 18001).

3.4. Costo de implementación del estándar ISO/IEC 27001:2005[J]

Según el experto en la norma ISO/IEC 27001, Dejan Kosutic[12], el costo de implementación de la ISO/IEC 27001:2005 es una de las primeras preguntas que se hacen los potenciales clientes, sin embargo no es posible proporcionar una cifra exacta ya que ante todo el costo total de la implementación depende del tamaño de la empresa o de las áreas que se encuentren dentro del alcance de la norma, del grado crítico de la información (por ejemplo, la información de los bancos se considera más crítica y requiere un nivel de protección mayor), de la tecnología que utiliza la organización (por ejemplo, los centros de datos suelen tener mayores costos debido a sus complejos sistemas) y de las disposiciones legales (generalmente, los sectores públicos y financieros están muy controlados en relación con la seguridad de la información).

En definitiva, sería imposible calcular los costos exactos antes de saber qué nivel de protección necesita la empresa, primero se debe realizar una evaluación de riesgos, ya que este análisis le mostrará qué medidas de seguridad necesita y luego se deberá tener en cuenta los siguientes costos:

- **Costo de publicaciones y de capacitación:** La implementación de la norma ISO/IEC 27001:2005[J] requiere cambios en la empresa y requiere también de nuevas capacidades a los empleados mediante la compra de libros sobre el tema y/o enviándolos a cursos (presenciales o en línea) de entre 1 a 5 días de duración. Además, se debe adquirir la norma ISO 27001[J] propiamente dicha ya que existen varios casos de empresas que están implementando la norma sin haberla visto realmente.

[12] Dejan Kosutic, *¿Cuánto cuesta la implementación de la norma ISO 27001?*, Febrero 2011, Internet. http://blog.iso27001standard.com/es/tag/iso-27001-es/, Acceso: marzo 2012

- **Costo de asistencia externa:** Muchas veces se requiere de la contratación de un consultor externo o asesorías en línea ya que por lo general las empresas no cuentan con un gerente de proyecto con experiencia en la implementación de la norma ISO/IEC 27001:2005[J]. Lo más valioso de tener alguien con experiencia que apoye en este tipo de proyectos es evitar terminar en callejones sin salida, que realmente cuestan (meses realizando actividades que no son realmente necesarias o trabajando con toneladas de documentación no requeridas por la norma). Sin embargo, no es una buena práctica esperar a que un consultor haga toda la implementación ya que solamente podrá ser implementada por sus empleados.

- **Costo de tecnología:** La mayoría de empresas en realidad no necesitan de grandes inversiones en hardware o software ya que disponen de estas, sin embargo el desafío está en conocer cómo utilizar la tecnología existente de forma más segura. A pesar de eso, sí es necesario planificar este tipo de inversiones en caso de ser necesarias.

- **Costo del tiempo de los empleados:** Debido a que la norma exige la participación de los empleados de la empresa en su implementación y funcionamiento, la empresa deberá asumir los costos por el tiempo que les tomará para identificar los riesgos, cómo mejorar los procedimientos y políticas existentes o implementar nuevas; sus capacitaciones y nuevas responsabilidades y para adaptarse a las nuevas normas.

- **Costo de la certificación:** El costo de la auditoría de certificación dependerá de la cantidad de días/hombre que le demande hacer el trabajo: podrá ser desde menos de 10 días/hombre para empresas pequeñas hasta unas docenas de días/hombre para empresas más grandes. El costo del día/hombre depende del mercado local. Las actividades de evaluación para la certificación de ISO/IEC 27001[J] por parte de un organismo de certificación acreditado, tendrán un costo de unos miles de dólares, más si la organización es extensa y compleja. También es necesario presupuestar el tiempo de la gerencia y del personal que ayudará a los auditores a solventar cualquier inconformidad importante que identifican que hay que resolver para obtener la certificación.

  La calidad de su SGSI y su preparación para la auditoría de certificación influye en el tiempo y por lo tanto los costos involucrados. Los niveles de estrés son generalmente más bajos si están bien preparados.

Se pueden organizar auditorías combinadas de múltiples sistemas, reduciendo el coste total, pero aumentando la complejidad y los problemas ocasionados. También serán necesarios seguimientos anuales y evaluaciones tri-anuales de recertificación, en contexto, son costos relativamente menores.

- **Costos Operativos y de mantenimiento:** Una vez que el SGSI está en marcha, habrán varios costos operativos y de mantenimiento, pero variarán de acuerdo a la naturaleza y el alcance del SGSI. Probablemente valga la pena diferenciar los costos de operación y mantenimiento de los relacionados con los controles de seguridad de la información gestionados, ya que los primeros tienen más probabilidades de ser discretos, mientras que los últimos tienden a ser requeridos en todo evento para limitar los riesgos de la organización.

- **Costos relacionados al cambio organizacional:** La implementación de un SGSI requiere una serie de cambios en las actividades de seguridad de información de la organización, mientras que la estabilidad y la estructura del SGSI puede hacer que inevitablemente estos cambios sean más difíciles. Las políticas, procedimientos y prácticas existentes relacionadas con la seguridad de la información tendrán que ser documentadas, revisadas y con frecuencia adaptadas al SGSI y con esto las prácticas de trabajo inseguras podrán ser eliminadas.

  Por otro lado, los ciclos de mejora continua de la norma ISO/IEC 27001[J] proporcionan un mecanismo de adaptación a los cambios más fácil y eficiente. Los empleados, proveedores o socios que constantemente o flagrantemente se nieguen a cumplir con los requisitos, políticas o procedimientos de la seguridad de la información pueden tener que ser despedidos, disciplinados, y / o procesados.

  Desde el punto de vista de la seguridad de la información, los cambios de esta naturaleza son positivos ya que prevén reducir el impacto de la seguridad de la información de la organización en el tiempo, a pesar de que causan interrupciones y costos de corto plazo a los departamentos y equipos que intervienen directamente. El SGSI proporciona el contexto, la información y los procesos para hacer frente a esto de manera estructurada.

Para el análisis costo beneficio, no se debe subestimar el costo real del proyecto de ISO/IEC 27001:2005[J] ya que la gerencia comenzará a ver el proyecto de forma negativa. Además, siempre se debe presentar tanto los costos como los beneficios de esta implementación.

3.5. Aplicación de la ISO/IEC 27001:2005[J]

Según Rodrigo Hiroshi Ruiz Suzuki, Consulting Manager de PromonLogicalis[13], el proyecto de implementación de la norma ISO/IEC 27001:2005[J] suele demorar entre 6 y 12 meses o más dependiendo del grado de madurez relacionado con la seguridad de la información y el alcance del SGSI que tiene la empresa. En general, se recomienda el apoyo de consultores externos para lograr este objetivo.

Aquellas empresas que hayan adecuado previamente las exigencias normativas y legales de protección de datos o hayan realizado acercamientos a la seguridad de la información en sus sistemas de información y procesos de trabajo, tendrán una ventaja a la hora de implementar el estándar.

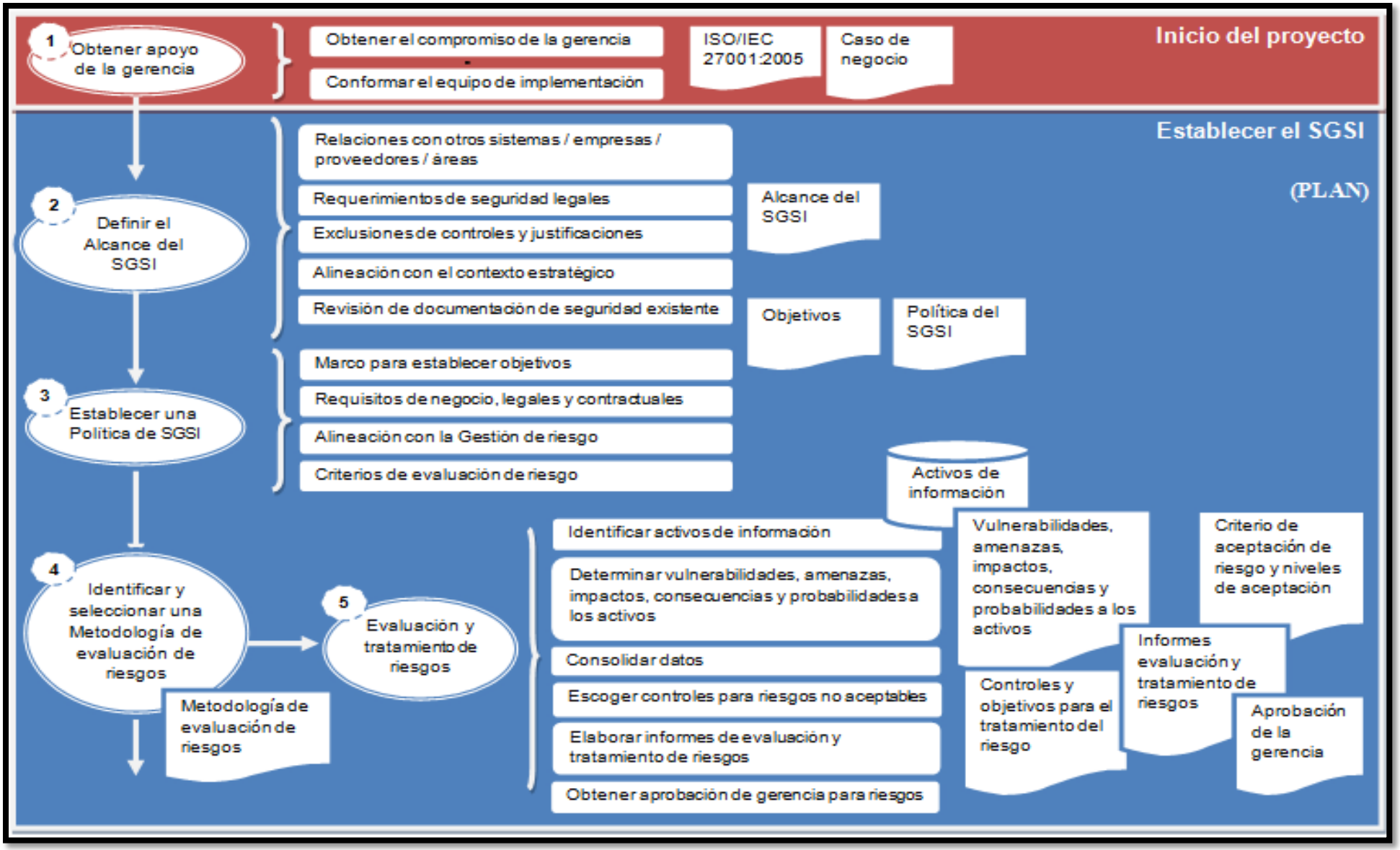
Implementar la ISO/IEC 27001:2005[J] requiere de una cuidadosa reflexión, planificación y coordinación que asegure una adaptación cómoda. La decisión acerca de cuándo y cómo implantar el estándar, puede verse influida por un número de factores que incluyen los distintos objetivos de negocio, los niveles actuales de madurez de TI y esfuerzos para la conformidad, aceptación y concienciación de los usuarios, necesidades de los clientes u obligaciones contractuales y la capacidad de la empresa de adaptación al cambio y adopción de los procesos internos.

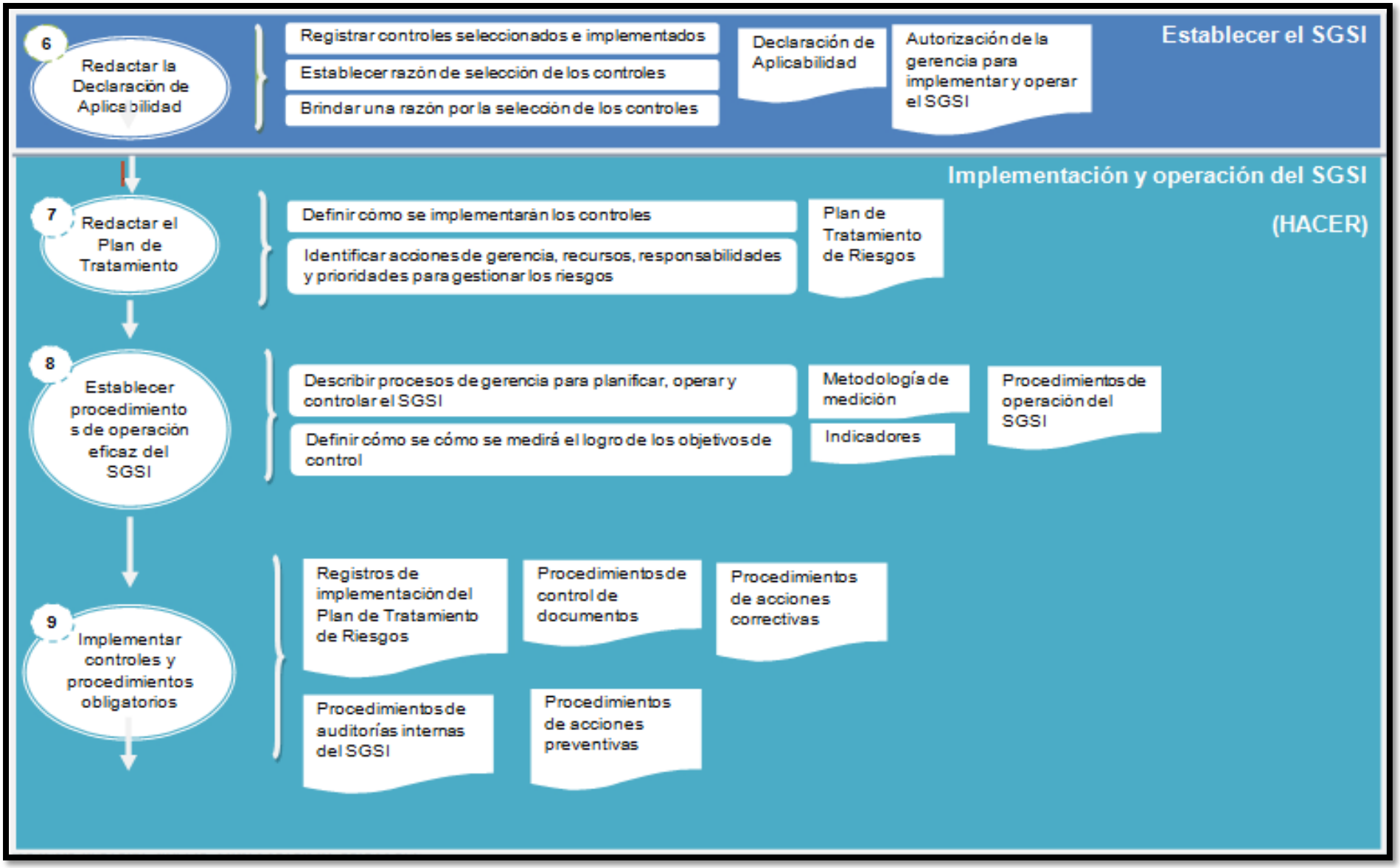
El gráfico a continuación[A], expone los pasos que habitualmente utilizan las empresas que han implantado un SGSI y posteriormente han certificado con éxito la ISO/IEC 27001[J][14]:

Para mayor detalle, ver Anexo B "Implementación de la ISO/IEC 27001:2005" adjunto este documento de Tesis.

[13] Rodrigo Hiroshi Ruiz Suzuki, *" ISO 27001, la norma que define como organizar la seguridad de la información en las organizaciones"*, *Logicalis Now*, marzo 2011, Internet, http://ebookbrowse.com/ln-13-12-certificaciones-iso27001-pag-51-53-pdf-d136991637 Acceso: marzo 2012.

[14] ISO27k Implementers' Forum, Versión 3 enero 2009, Internet, http://www.iso27001security.com/ISO27k_ISMS_implementation_and_certification_process_v3.pdf, Acceso: marzo 2012


Inicio del proyecto
1 Obtener apoyo de la gerencia
Obtener el compromiso de la gerencia
Conformar el equipo de implementación
ISO/IEC 27001:2005
Caso de negocio
Establecer el SGSI
(PLAN)
2 Definir el Alcance del SGSI
Relaciones con otros sistemas / empresas / proveedores / áreas
Requerimientos de seguridad legales
Exclusiones de controles y justificaciones
Alineación con el contexto estratégico
Revisión de documentación de seguridad existente
Alcance del SGSI
3 Establecer una Política de SGSI
Marco para establecer objetivos
Requisitos de negocio, legales y contractuales
Alineación con la Gestión de riesgo
Criterios de evaluación de riesgo
Objetivos
Política del SGSI
4 Identificar y seleccionar una Metodología de evaluación de riesgos
Metodología de evaluación de riesgos
5 Evaluación y tratamiento de riesgos
Identificar activos de información
Determinar vulnerabilidades, amenazas, impactos, consecuencias y probabilidades a los activos
Consolidar datos
Escoger controles para riesgos no aceptables
Elaborar informes de evaluación y tratamiento de riesgos
Obtener aprobación de gerencia para riesgos
Activos de información
Vulnerabilidades, amenazas, impactos, consecuencias y probabilidades a los activos
Criterio de aceptación de riesgo y niveles de aceptación
Controles y objetivos para el tratamiento del riesgo
Informes evaluación y tratamiento de riesgos
Aprobación de la gerencia


Establecer el SGSI
6
Redactar la Declaración de Aplicabilidad
Registrar controles seleccionados e implementados
Establecer razón de selección de los controles
Brindar una razón por la selección de los controles
Declaración de Aplicabilidad
Autorización de la gerencia para implementar y operar el SGSI
Implementación y operación del SGSI
(HACER)
7
Redactar el Plan de Tratamiento
Definir cómo se implementarán los controles
Identificar acciones de gerencia, recursos, responsabilidades y prioridades para gestionar los riesgos
Plan de Tratamiento de Riesgos
8
Establecer procedimientos de operación eficaz del SGSI
Describir procesos de gerencia para planificar, operar y controlar el SGSI
Definir cómo se cómo se medirá el logro de los objetivos de control
Metodología de medición
Indicadores
Procedimientos de operación del SGSI
9
Implementar controles y procedimientos obligatorios
Registros de implementación del Plan de Tratamiento de Riesgos
Procedimientos de control de documentos
Procedimientos de acciones correctivas
Procedimientos de auditorías internas del SGSI
Procedimientos de acciones preventivas

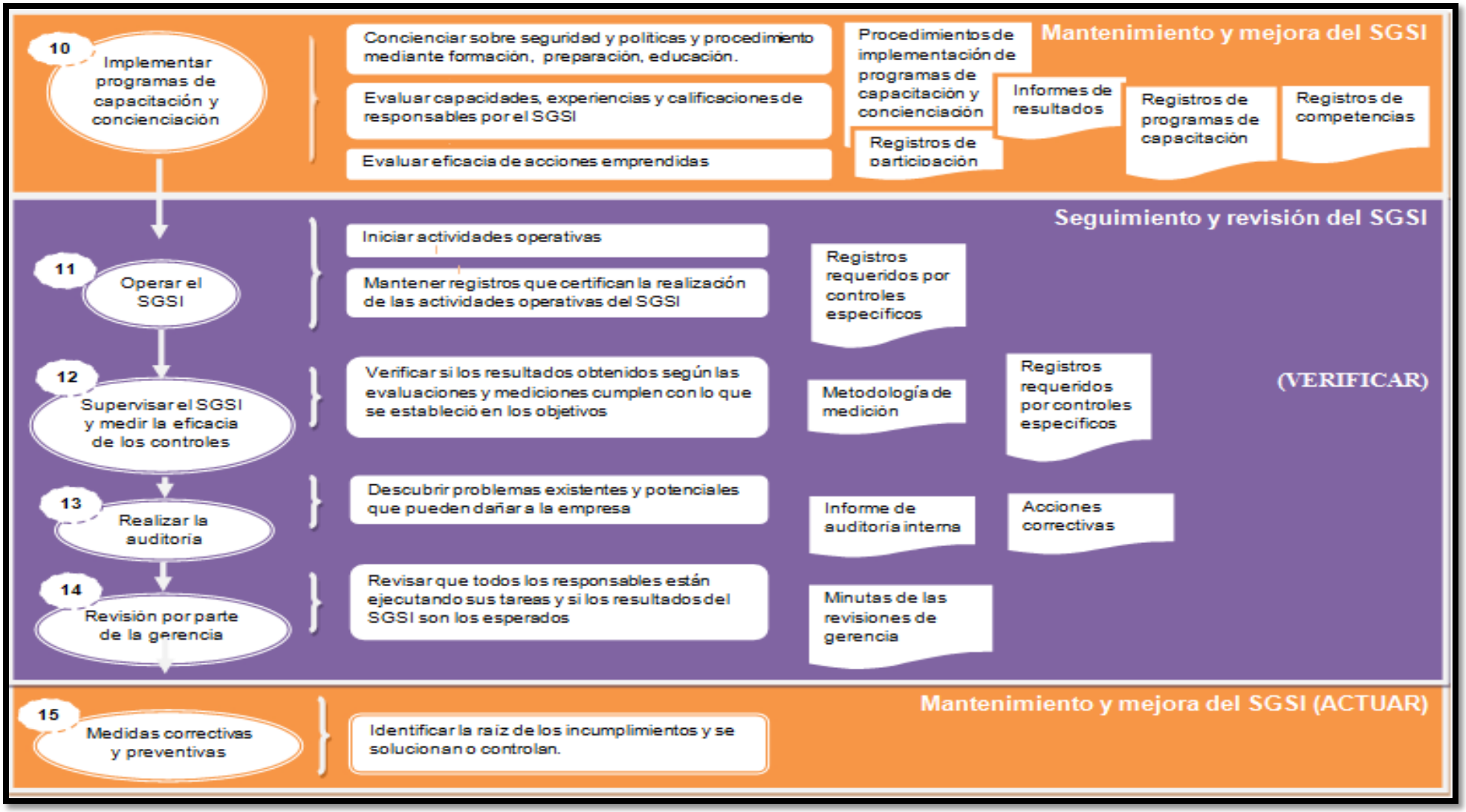


Figura 3-03 Pasos para la implementación de la ISO/IEC 27001:2005[J]

3.6. Certificación de la ISO/IEC 27001:2005[J]

El tema de la certificación en aspectos de seguridad de información aún no ha sido considerado con la seriedad que se merece en el ámbito empresarial, sin embargo no hay duda que en el muy corto plazo será una cuestión importante e incluso obligatoria para cualquier empresa que desee competir en el mercado, lo cual es lógico, pues para interrelacionar infraestructuras de información entre empresas, se deben exigir mutuamente niveles concretos y adecuados de seguridad.

Una de las grandes ventajas para una empresa certificada, es su reconocimiento externo. Disponer de una certificación significa que una tercera parte independiente y acreditada avala que los niveles del SGSI cumplen con los estándares internacionalmente aceptados de buenas prácticas para la gestión de la seguridad de la información.

Aquellas empresas que hayan completado con éxito el proceso de certificación pueden obtener una mayor confianza en su capacidad para gestionar la seguridad de la información. Una vez que la empresa disponga de la documentación y procesos que exige la norma, deberá hacer una solicitud a la Entidad de Certificación para el inicio del proceso de la auditoría.

En Ecuador no existe una Entidad de Certificación formal. La primera empresa ecuatoriana certificada es Telconet y su entidad de certificación fue internacional: SGS United Kingdom. Movistar que también se certificó en febrero 2012, fue auditada por la Asociación Española de Normalización y Certificación AENOR.

Para aprobar una acreditación la Entidad Certificadora realiza una auditoría en dos fases[L] :

3.6.1. FASE 1: Revisión de la documentación:

Uno de los objetivos de la auditoría fase 1 es la revisión de la documentación que exige la norma, la cual permite a la Entidad de Certificación la comprensión del SGSI dentro del contexto de la política de seguridad, objetivos y aproximación a la gestión de riesgos de la empresa. En esta fase, el auditor buscará la documentación mínima requerida por la norma y los registros sobre los controles del Anexo A de la norma ISO/IEC 27001:2005[j], el cual enumera en un cuadro los objetivos de control y controles detallados en la norma ISO 27002:2005[j], incluidos en la Declaración de Aplicabilidad.

[L] Ramón Robles, Álvaro Rodriguez de Roa, *La gestión de la Seguridad en la empresa*, Revista Q, pág. 17, junio 2006.

Ésta fase sirve como punto de referencia útil a la hora de preparar la auditoría de fase 2 y ofrece una oportunidad para evaluar el grado de preparación de la empresa. Si falta alguno de estos elementos, significa que la empresa no está lista para la Fase 2 de auditoría. Dicha fase puede complementarse, en función de la complejidad del SGSI, con una visita a las instalaciones de la empresa para comprobar y aclarar aspectos del SGSI que sean requisitos obligatorios para el éxito de la auditoría de certificación.

3.6.2. FASE 2: Auditoría "in situ"

Esta auditoría también es conocida como 'auditoría principal' y está guiada por las conclusiones del informe de auditoría de fase 1. Se redactará el plan de auditoría basándose en estas conclusiones y se enviará con la debida antelación a la empresa proponiendo el equipo auditor, itinerario, tiempos, recursos necesarios, entre otros. En la fecha programada se llevará a cabo la auditoría en las instalaciones de la organización donde esté desplegado e implantado el SGSI.

El enfoque de esta auditoría no se trata de la documentación si no sobre si la empresa realmente está haciendo lo que sus documentos y la norma indican qué hacer. Es decir que se hará una verificación sobre si el SGSI se aplica o está solamente en letra muerta mediante entrevistas con el personal de la empresa y control de los registros presentados. Entre los registros obligatorios se incluyen los de formación, capacitación, habilidades, experiencias y calificaciones, auditoría interna, revisión por parte de la gerencia y medidas correctivas y preventivas. Sin embargo, el auditor esperará ver muchos más registros como resultado de la realización de los procedimientos tanto obligatorios como los que no son mandatorios.

Aunque el auditor encuentre alguna falla grave que impida la obtención de la certificación, todavía hay una oportunidad. El procedimiento en este caso es el siguiente: el auditor informará los resultados incluyendo el incumplimiento en un periodo de aproximadamente 90 días. El trabajo de la empresa es tomar las medidas correctivas correspondientes teniendo el cuidado de que estas medidas deben atacar al origen del incumplimiento, caso contrario el auditor no aceptará las acciones llevadas a cabo.

Una vez tomadas las medidas correctivas, la empresa debe notificar al auditor y hacerle llegar las evidencias del caso para que decida aceptar los cambios y active el proceso de emisión del certificado.

Se debe tomar en cuenta que el certificado tiene una duración de tres años (al tercer año se hace una auditoría de recertificación) pudiendo ser suspendido durante este periodo si la Entidad Certificadora detecta algún otro incumplimiento grave en sus visitas de control y seguimiento realizadas semestral o al menos anualmente .

Como conclusión del presente capítulo, hemos visto que la ISO/IEC 27001:2005[J] representa un cambio en la manera de afrontar la seguridad de la información en las empresas, mediante un modelo formal, estandarizado, documentado, iterativo y global. Su implementación puede presentar complejidades y de igual manera tiene un costo para la empresa que no siempre es fácil de justificar a la dirección, por lo que en este capítulo presentamos la información y procedimientos a ser tomados en cuenta para que el proyecto de implementación y certificación resulte más sencillo, su ejecución más rápida y con un impacto razonable en costos.

CAPÍTULO IV: PROCEDIMIENTO PARA EL ANÁLISIS COSTO BENEFICIO

Actualmente muchas personas, especialmente de la alta gerencia, no han comprendido la importancia estratégica que tiene la explotación adecuada de la información y su seguridad para el alcance de resultados organizacionales de excelencia. Una de las herramientas a través de la cual se puede entender el beneficio de invertir en la seguridad de la información de los activos más importantes en su empresa y de determinar si los costos pueden o no estar justificados por los resultados y efectos de las acciones implementadas, es el Análisis Costo Beneficio.

"Para la identificación de los costos y beneficios del proyecto que son pertinentes para su evaluación, es necesario definir una situación base o situación sin proyecto; la comparación de lo que sucede con proyecto versus lo que hubiera sucedido sin proyecto, definirá los costos y beneficios pertinentes del mismo". [M]

En el presente capítulo, plantearemos el procedimiento y la teoría que se seguirá en el capítulo VI para el análisis costo beneficio de la aplicación del Estándar ISO/IEC 27001:2005 a la empresa seleccionada.

4.1. Fases para el análisis Costo Beneficio

El Análisis Costo Beneficio permite a la gerencia identificar las ganancias o pérdidas potenciales de una propuesta de proyecto, convertirlas en unidades monetarias y tomar una decisión sobre el curso de acción de los resultados.

A nivel general, se seguirán los siguientes pasos para llegar al cálculo del Costo Beneficio de la aplicación del Estándar ISO/IEC 27001:2005 en una empresa industrial[15]:

1. **Visión general de la seguridad de la información en la empresa seleccionada.** Se presenta un análisis general de la organización, conociendo su historia, información estratégica, estructura general, la descripción general del negocio y su crecimiento durante los últimos diez años, además de la situación general de la seguridad de la empresa respecto y un comparativo con la III encuesta Latinoamericana de seguridad de la información.

   El detalle de esta primera fase se encuentra en el capítulo V "Situación Actual de la seguridad de la información en la empresa seleccionada".

2. **Recopilación de información sobre activos de información de la empresa**. A través de reuniones con usuarios claves en la empresa seleccionada, se obtiene información referente a los activos de información de la misma. Durante esta fase se recopila información general, como:
   1. Descripción de los activos de información en la empresa
      - Nombre del activo
      - Localización del activo en la empresa
      - Propietario responsable del activo
   2. Clasificación de los Activos[1]
      - Clase de Activo
      - Entorno Global de TI
   3. Incidentes de seguridad relacionados con los activos de información
      - Descripción del incidente
      - Costo que el incidente implicó
   4. Niveles de defensa de los activos de información[1]
   5. Nivel de impacto del activo para el Negocio[1]
   6. Amenazas de seguridad de los activos[1]
   7. Vulnerabilidades de los activos[1]
   8. Nivel de exposición de los activos[1]

El detalle de esta primera fase se encuentra en el punto "4.3. Recopilación de datos sobre activos de información de la empresa" del presente capítulo.

3. **Evaluación de riesgos cualititativa y cuantitativa [1].** La evaluación de riesgos consiste en identificar de manera resumida el impacto de las vulnerabilidades y amenazas asociadas a cada activo de información recopilado en la primera fase, que puede provocar sobre la disponibilidad de los mismos.[E] La evaluación de riesgos es necesaria para determinar cuánto una empresa debe invertir en Seguridad de Información. En otras palabras, la evaluación de riesgos ayuda a calcular la pérdida financiera (costo) ocasionada por incidentes de seguridad, además permite calcular el beneficio de la medida de mitigación de los riesgos identificados (beneficio).

   Existen diversas metodologías de evaluación de riesgos (MAGERIT[C], OCTAVE, AS/NZS, BS7799-3:2006, ISO/IEC 27005:2008), e incluso herramientas que ayudan a automatizar el proceso (EAR/PILAR), que siguen una secuencia de acción muy similar, por lo que la selección de una metodología queda a discreción de la persona que va a ser uso de esta y entre otros debería cubrir los siguientes puntos:

   1. Evaluar las amenazas sobre los activos identificados previamente y su probabilidad de que sucedan.
   2. Valorar las vulnerabilidades de los activos, las cuales pueden ser explotadas por las amenazas.
   3. Valorar el impacto resultante de que una amenaza se aproveche de una vulnerabilidad del activo y provoque daño sobre el mismo.
   4. Calcular el riesgo como la probabilidad de que se produzca un impacto determinado en la organización.

   Independientemente de la metodología o de las herramientas empleadas para el análisis de riesgos, el resultado del proceso será un mapa de riesgos que permite identificar y priorizar aquellos que pueden provocar una paralización de las actividades de negocio de la organización o de los recursos críticos sobre los cuales dichas actividades están soportadas. Para el caso del presente trabajo de Tesis, se ha determinado utilizar la Evaluación de Riesgos que propone la Guía de Administración de Riesgos de Microsoft.[1]

El proceso de Evaluación de Riesgos de la Guía de Administración de Riesgos de Seguridad de Microsoft[1] primero aplica un enfoque cualitativo para identificar y asignar prioridades a los riesgos. Luego para determinar el Costo Beneficio de la estrategia de mitigación de riesgos se aplica un enfoque cuantitativo, seleccionando los riesgos de prioridad alta y moderada de la evaluación cualitativa con la estimación de su posible costo monetario. En el siguiente cuadro se describen los dos tipos de evaluaciones junto con las ventajas e inconvenientes asociados a los mismos.

Tipo de Análisis de Riesgos	Descripción	Ventajas	Inconvenientes
Cualitativo	Basado en clasificaciones descriptivas y subjetivas del riesgo	• Sencillez • Rapidez • Equilibrio Coste-Beneficio • Uso extendido	Subjetividad
Cuantitativo	Basado en términos monetarios	• Exactitud • Objetividad	Complejidad para estimar costes reales

Cuadro 4-01 Descripción de Tipos de Evaluación de Riesgos[E]

4. **Análisis Costo Beneficio.** En esta fase se realizará una comparación entre los costos y los beneficios de la implementación de la ISO/IEC 2007:2005. Para esto se procederá a sumar los costos totales de cada activo de información sin la aplicación del estándar ISO/IEC 27001:2005[J] y luego sumar la proyección de los costos con la aplicación del estándar ISO/IEC 27001:2005[J], más el costo de su implementación (controles). Comparar, a través de ROSI[25] las relaciones Beneficios a Costos y sacar las respectivas conclusiones.

   En el peor de los casos, una empresa no debería invertir en un proyecto que resulte más costoso que la pérdida que pudiera sufrir por no implementar dicho proyecto.[7]

[E] Inteco – Deloitte, *Guía para PYMES, Cómo Implantar un Plan de Continuidad del Negocio*, 2010, página 37.

[25] ROSI: Return of Security Investment o Retorno de la Inversión en Seguridad

El detalle de esta tercera fase se encuentra en el punto "4.4. Evaluación Costo Beneficio" del presente capítulo.

A continuación se detallarán cada una de las fases para la obtención del Análsis Beneficio de la aplicación de la ISO/IEC 27001:2005.

4.2. Visión general de la seguridad de información en la empresa seleccionada

La explicación detallada de la información general de la empresa y los temas relevantes con la seguridad de la información, se ha destinado todo el capítulo V del presente trabajo.

4.3. Recopilación de información sobre activos de información de la empresa

La presencia de los activos de información facilita el funcionamiento de la empresa y la consecuencia de sus objetivos. Según la Guía de Administración de Riesgos de Seguridad de Microsoft[1], los principales elementos a recopilar durante esta fase son:

1. **Realizar la descripción de los activos:** Breve explicación de cada activo, su responsabilidad y ubicación, para facilitar la comprensión común en la fase de evaluación de riesgos.

2. **Asignar la clase de activo de información:** Un activo es cualquier servicio o elemento tangible o intangible que represente un valor para la empresa. Se utiliza la siguiente clasificación de activos:

Clase de Activo	Entorno Global de TI
Servicios	Infraestructura Básica
	Mensajería
	Otra Infraestructura
Tangibles	Datos de Intranet
	Datos de Internet
	Datos de Extranet
	Infraestructura física
	Personal
	Personal Tecnología
Intangible	Productividad de empleados
	Buena Voluntad
	Moral de empleados
	Reputación

Cuadro 4-02 Clasificación de Activos[1]

3. **Identificar incidentes de seguridad relacionados a cada uno de los activos de información:** Para facilitar la estimación la probabilidad de ocurrencia en la evaluación de riesgos, se hace un levantamiento de incidentes suscitados en la empresa, atados a los activos de información que apliquen. Además se asocian los costos ocasionados por los incidentes para valorar la magnitud del incidente en valores monetarios.

4. **Establecer niveles de defensa de los activos:** Para facilitar la detección de riesgos y aplicación de los controles adecuados, se han clasificado las amenazas y vulnerabilidades según los niveles de defensa que propone la Evaluación de Riesgos de la Guía de Administración de Riesgos de Microsoft[1]. Esta organización proporciona una estructura y facilita la recopilación de riesgos en la empresa. Un activo de información puede tener varios niveles de defensa. Los niveles de defensa son:

Nivel de defensa	Descripción
1: Físicas	Protecciones, seguros, dispositivos de seguimiento.
2: Defensas en la Red	La implementación de defensas de red internas incluye la consideración del diseño de red adecuado, la seguridad de red inalámbrica para garantizar que sólo los equipos de confianza tengan acceso a los recursos de red críticos, segmentos de red.
3: Defensas de Host	Los hosts son de 2 tipos: clientes y servidores. Las defensas de host pueden incluir deshabilitar servicios, quitar derechos de usuario específicos, mantener actualizado el sistema operativo, así como utilizar antivirus y productos de servidor de seguridad distribuidos.
4: Defensas de Aplicación	La implementación de las defensas de aplicación incluye una arquitectura de aplicaciones correcta, incluida la garantía de que la aplicación se ejecuta con el mínimo nivel de privilegio con la menor superficie de ataque expuesta posible.
5: Defensas de Datos	Los datos se pueden proteger de diferentes maneras, a través de contraseñas fuertes, ACLs, estrategias de respaldo y restauración, uso del servicio de archivos de cifrado (EFS).

Cuadro 4-03 Niveles de Defensa [1]

5. **Definir el Nivel de Impacto del activo para el negocio:** El impacto para el negocio puede ser (HBI[26]:Alto, MBI[27]:Moderado y LBI[28]:Bajo) definido en base al nivel de impacto de pérdidas que estos activos pueden provocar sobre la organización, basados en los siguientes criterios, planteados por la Evaluación de Riesgos de la Guía de Administración de Riesgos de Microsoft[1] :

[26] HBI: High Business Impact
[27] MBI: Moderate Business Impact
[28] Low Business Impact

Clase de Activo por Impacto al Negocio		Descripción
10	**HBI: Impacto al Negocio Alto**	El impacto en la confidencialidad, la integridad o la disponibilidad de estos activos provocan pérdidas graves o catastróficas para la organización. Los impactos se pueden expresar en términos financieros puros o pueden reflejar pérdida indirecta o robo de instrumentos financieros, productividad de la organización, daños a la reputación o responsabilidad legal o normativa importante
5	**MBI: Impacto al Negocio Medio**	El impacto en la confidencialidad, la integridad o la disponibilidad de estos activos provocan pérdidas moderadas para la organización. La pérdida moderada no constituye una repercusión grave o catastrófica, pero altera las funciones organizativas normales hasta el punto de que son necesarios controles proactivos para minimizar los impactos en esta clase de activos.
2	**LBI: Impacto al Negocio Bajo**	Los activos que no son de impacto alto o de impacto moderado tienen la clasificación de impacto bajo en la empresa y no tienen requisitos de protección formales ni controles adicionales aparte de las prácticas recomendadas estándar para proteger la infraestructura

Cuadro 4-04 Clasificación de Activos según el impacto al negocio[1]

6. **Establecer Amenazas de seguridad:** Identificar las causas o sucesos que pueden afectar negativamente a un activo, representados por su pérdida de confidencialidad, integridad o disponibilidad.

7. **Definir Vulnerabilidades:** Establecer los puntos débiles o ausencia de controles que se pueden aprovechar para atacar un activo.

8. **Identificar el Nivel de exposición:** Para la estimación del alcance de los daños posibles al activo, la guía recomienda pedir a los participantes que seleccionen un nivel de exposición alta, moderada o baja y registrarla.

Nivel de Exposición	Descripción
Alta	Pérdida severa o completa del activo
Moderada	Pérdida limitada o moderada del activo
Baja	Pérdida mínima o nula del activo

Cuadro 4-05 Nivel de exposición de Activos de Información [1]

4.4. Evaluación de Riesgos cualitativa y cuantitativa

A continuación, se proporciona un detalle sobre los pasos a seguir para realizar una evaluación de riesgos cualitativa y cuantitativa.

4.4.1. Evaluación de Riesgos Cualitativa

Para esta etapa de la evaluación de riesgos se asignan calificaciones relativas a activos, vulnerabilidades, amenazas y riesgos. Su fundamento teórico se basa en lo mencionado en el capítulo II, respecto a que el Riesgo es la probabilidad de que una amenaza explote una vulnerabilidad asociada a un activo. El riesgo cualitativo es producto de las entradas en la matriz de evaluación de riesgos, en función de:

MATRIZ [Impacto, Probabilidad]

Donde:

- Impacto = f (criticidad del activo, gravedad de la vulnerabilidad). Posibles valores: alto, moderado o bajo.
- Probabilidad = f (frecuencia de la amenaza, facilidad de explotación de la vulnerabilidad). Posibles valores: alto, moderado o bajo.

A continuación, se proporciona un detalle de los pasos involucrados en cada una de las fases de la evaluación de riesgos cualitativa, que permitirá obtener la evaluación resumida de los activos:

1. **Determinar el impacto:** El impacto se determinará a partir de la información proporcionada en el proceso de recopilación de datos (4.2). La clasificación del activo por el Impacto al Negocio y Nivel de Exposición obtenida en el proceso de recopilación de datos se debe resumir en un solo dato para determinar el impacto.

MATRIZ_IMPACTO [Impacto al negocio, Nivel de exposición]

El siguiente cuadro se utiliza para seleccionar el nivel por cada declaración de impacto:

		Impacto		
Clase de activo por Impacto al Negocio *(4-04)*	**10**	Impacto moderado	Impacto alto	Impacto alto
	5	Impacto bajo	Impacto moderado	Impacto alto
	2	Impacto bajo	Impacto bajo	Impacto moderado
		Bajo	**Moderado**	**Alto**
		Nivel de exposición *(4-05)*		

Cuadro 4-06 Impacto por Clase de Activo y Nivel de Exposición[1]

2. **Estimar la probabilidad del impacto.** Las categorías de probabilidad se incluyen a continuación como referencia:

Probabilidad	Descripción
Alta	Muy probable, se esperan uno o varios impactos en un año.
Media	Probable, se espera un impacto de dos a tres años.
Baja	No probable, no se espera que ocurra ningún impacto en tres años.

Cuadro 4-07 Probabilidad de ocurrencia del impacto[1]

3. **Asignar el nivel de riesgos.** El nivel de riesgos es el resultado de la combinación de los valores de impacto (4-06) y de probabilidad (4-07) obtenidos previamente. Se utiliza el siguiente cuadro para seleccionar el nivel de riesgo.

MATRIZ_RIESGO [Probabilidad, Impacto]

		Riesgo		
Impacto *(4-06)*	**Alto**	Riesgo moderado	Riesgo alto	Riesgo alto
	Moderado	Riesgo bajo	Riesgo moderado	Riesgo alto
	Bajo	Riesgo bajo	Riesgo bajo	Riesgo moderado
		Baja	**Media**	**Alta**
		Probabilidad *(4-07)*		

Cuadro 4-08 Nivel de Riesgo resumido[1]

4. **Selección de riesgos para nivel detallado.** El resultado final es una lista resumida de niveles de riesgos de cada activo, priorizando aquellos que requieren de una medida de mitigación más exhaustiva y con mayor urgencia, para lo cual se aplica el siguiente criterio:

Nivel de Riesgo	Acción a tomar
Alto	Incluir en el análisis detallado. Todos los riesgos altos deben tener una medida de mitigación urgente.
Moderado	Incluir en el análisis detallado a aquellos riesgos moderados que requieren de una medida de mitigación urgente.
Bajo	No incluir en el análisis detallado y considerarlos para una siguiente etapa.

Cuadro 4-09 Criterio para seleccionar riesgos para nivel detallado[1]

5. **Definición de controles de acuerdo a la norma ISO/IEC 27001:2005:** Para cada uno de los activos y sus niveles de defensa seleccionados para la medición detallada, se requiere la definición de los controles a implementar basados en el Anexo A de la norma ISO/IEC 27001:2005. Esta fase es fundamental dentro del análisis costo beneficio por cuanto de este punto en adelante las mediciones que se realicen serán en función de comparar los resultados sin la implementación de controles y con la implementación de controles. Adicionalmente para completar esta etapa en vista de que los controles de la norma son bastante generales se sugiere el proyecto a desarrollar.

6. **Determinar el nivel de exposición detallado por cada activo de información.** El nivel de exposición detallado contiene mayor granularidad con respecto al nivel de exposición determinado durante la etapa de recopilación de información *(punto 4.2)*, conteniendo 2 criterios, cada uno con 5 valores de clasificación basados en Confidencialidad e Integridad y Disponibilidad de la información.

   La Guía de Administración de Riesgos de Microsoft[1] recomienda utilizar los criterios de los cuadros 4-10 y 4-11 como orientación para determinar el nivel de exposición adecuado.

   1. El primer criterio de exposición reflejado en el cuadro 4-10 ayuda a cuantificar el alcance de los impactos de un ataque a la confidencialidad e integridad de los activos:

Nivel de exposición detallado	Confidencialidad e integridad de Activos *(primer criterio)*
5	Daños graves o totales al activo; son visibles externamente y afectan a la rentabilidad o al éxito de la empresa
4	Daños graves, pero no totales al activo; afectan a la rentabilidad o al éxito de la empresa, pueden ser visibles externamente.
3	Pérdida o daños moderados; afectan a prácticas de negocios internas, se produce un aumento de los costos operativos o se reducen los ingresos
2	Daños o pérdida moderados; afectan a las prácticas de negocios internas, no se puede medir un aumento de los costos

Nivel de exposición detallado	Confidencialidad e integridad de Activos *(primer criterio)*
1	Cambios menores en el activo o ningún cambio

Cuadro 4-10 Primer criterio para el Nivel de Exposición, basado en la confidencialidad e integridad de la información[1]

2. El segundo criterio de nivel de exposición reflejado en el cuadro 4-11, ayuda a cuantificar los impactos en la disponibilidad de los activos.

Nivel de exposición detallado	Disponibilidad *(segundo criterio)*	Descripción
5	Detención del trabajo	Importantes costos de soporte técnico o compromisos de negocios cancelados
4	Interrupción del trabajo	Aumento cuantificable de los costos de soporte técnico o retraso en los compromisos de negocios
3	Retrasos en el trabajo	Efecto apreciable en los costos de soporte técnico y en la productividad. No se producen consecuencias en la empresa que se puedan medir
2	Distracción en el trabajo	No se puede medir el efecto, pequeños aumentos en los costos de soporte técnico o de infraestructura
1	Absorbidos por las operaciones de negocios normales	Sin impacto cuantificable en los costos de soporte técnico, productividad o compromisos de negocios

Cuadro 4-11 Segundo criterio para calcular el Nivel de Exposición, basado en la disponibilidad de la información[1]

Para obtener un solo valor a partir de los dos criterios empleados en la determinación del nivel de exposición, la Guía de Administración de Riesgos de Microsoft[1] sugiere seleccionar el mayor valor entre los dos criterios seleccionados.

7. **Determinar el nivel de impacto detallado por cada activo de información:** Después de haber determinado el nivel de exposición detallado, la Guía de Administración de Riesgos de Microsoft[1] propone calcular para cada activo el nivel de impacto detallado, el cual representa el producto del Impacto al Negocio (4-04) identificado en la fase de recopilación de información (4.2) con el Factor de Exposición (4-12), el cual determina el porcentaje del daño en el activo cuando se materializa la amenaza identificada (si consideraría que la amenaza daña la totalidad del activo, el factor de exposición sería del 100%). El resultado del nivel de impacto detallado puede ir del 0 al 10.

   El cuadro 4-12 expone el Factor de Exposición como una equivalencia con el Nivel de Exposición calculado en el paso anterior (valor mayor entre los dos criterios expuestos en los cuadros 4-10 y 4-11):

Nivel de Exposición *(mayor valor entre 4-10 y 4-11)*	**Factor de Exposición (%)** *(Equivalencia en porcentaje del nivel de exposición)*
5	100%
4	80%
3	60%
2	40%
1	20%

Cuadro 4-12 Factor de Exposición [1]

El cuadro 4-13 hace una equivalencia entre el Nivel de Impacto al Negocio resumido (4-04) y el Nivel de Impacto detallado a obtener. El Nivel de Impacto Detallado puede tener un rango de valores de 0 a 10.

Nivel de Impacto al Negocio Resumido *(4-04)*	**Nivel de Impacto Detallado** *(4-04 * 4-12)*
10 – Alto	7 – 10
5 – Moderado	4 – 6
2 – Bajo	0 – 3

Cuadro 4-13 Nivel de Impacto Detallado [1]

8. **Determinar la probabilidad del impacto detallado por cada activo de información:** Según la Guía de Administración de Riesgos de Microsoft[1], la clasificación de probabilidad de ocurrencia consta de dos valores:

    1. El primer valor determina la probabilidad de ocurrencia de la vulnerabilidad existente en el *entorno* según los atributos de la misma y al ataque posible.
    2. El segundo valor determina la probabilidad de ocurrencia de la vulnerabilidad existente en función de la efectividad de los *controles actuales*. Cada valor se representa mediante un intervalo de 1 a 5.

    La Guía de Administración de Riesgos de Microsoft[1] recomienda utilizar la plantilla en el cuadro 4-14 como orientación para determinar la probabilidad de ocurrencia de cada impacto en la organización. La Guía emplea los siguientes criterios de vulnerabilidad:

    - **Población de piratas informáticos:** la probabilidad de ataque normalmente aumenta a medida que se incrementa el tamaño y el nivel de conocimientos técnicos de la población de piratas informáticos.
    - **Acceso remoto y local:** la probabilidad normalmente aumenta si una vulnerabilidad se puede aprovechar de forma remota.
    - **Visibilidad de vulnerabilidad:** la probabilidad normalmente aumenta si una vulnerabilidad es conocida y está disponible de forma pública.
    - **Automatización de ataque:** la probabilidad normalmente aumenta si un ataque se puede programar para buscar automáticamente vulnerabilidades en entornos grandes.

Atributos de Probabilidad de ocurrencia de las vulnerabilidades en su entorno *(seleccionar una)*	
Alta (Calificar con "5" si cualquiera aplica) • Existe una población grande de atacantes (aficionados) • Se puede ejecutar de forma remota • Se necesitan privilegios anónimos • Método de aprovechamiento publicado externamente • Automatizado	
Media (Calificar con "3" si cualquiera aplica) • Existe una población mediana de atacantes (expertos especialistas) • No se puede ejecutar remotamente • Se necesitan privilegios de nivel de usuario • Método de aprovechamiento no público • No automatizado	
Baja (Calificar con "1" si cualquiera aplica) • Existe una población pequeña de atacantes (conocimiento interno) • No se puede ejecutar remotamente • Se necesitan privilegios de nivel de administrador • Método de aprovechamiento no público • No automatizado	
[A]=Probabilidad de ocurrencia de la vulnerabilidad *(según su entorno)*	***(1, 3 o 5)***
Atributos de Probabilidad de ocurrencia para las Vulnerabilidades según la efectividad de sus controles	Calificación *(SI = 1; NO = 0)*
¿El control se ha definido y cumplido de forma eficaz?	
¿La toma de conciencia se comunica y sigue de forma eficaz?	
¿Los procesos se han definido y puesto en práctica de forma eficaz?	
¿La tecnología o los controles existentes reducen la amenaza de forma eficaz?	
¿Son suficientes las prácticas de auditoría actuales para detectar abusos o deficiencias de control?	
[B] = Probabilidad de ocurrencia de la vulnerabilidad *(según la efectividad de sus controles)*	**Σ** ***(0 - 5)***
Probabilidad de ocurrencia del Impacto	**[A]+[B]** ***(1 - 10)***

Cuadro 4-14 Plantilla para el cálculo de la Probabilidad de Impacto[1]

9. **Determinar el nivel de riesgo detallado:** El nivel de riesgo es el producto de la clasificación del nivel de exposición (1 - 10) y la probabilidad del impacto (0 - 10). De este modo se genera un intervalo de valores de 0 a 100.

   En el siguiente cuadro se muestra la combinación entre el nivel de exposición y la probabilidad de impacto para determinar el nivel de cada riesgo identificado.

		Nivel de Riesgo Detallado										
Nivel de Impacto *(4-13)*	**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
	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
	1	0	1	2	3	4	5	6	7	8	9	10
		0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
		Probabilidad de ocurrencia del impacto *(4-14)*										

Cuadro 4-15 Nivel de Riesgo Detallado[1]

Además, se presenta un cuadro de equivalencia cualitativa:

Nivel de Riesgo Detallado	Equivalencia
41-100	Alto
20-40	Moderado
0-19	Bajo

Cuadro 4-16 Equivalencia Cualitativa Nivel de Riesgo Detallado[1]

4.4.2. Evaluación de Riesgos Cuantitativa

El objetivo de la evaluación de riesgos cuantitativa es valorar el costo posible los activos con nivel de riesgo detallado ALTO y MODERADO determinados durante la evaluación de riesgos cualitativa. El valor de cada activo se calcula en función de lo que costaría reemplazarlo, lo que costaría en pérdida de productividad, lo que costaría en reputación de marca y en otros valores de negocios directos e indirectos.

A continuación se presentan los 3 grandes pasos generales a seguir en una evaluación de riesgos cuantitativa:

1. **Asignar un valor monetario a cada clase de activos de la organización (VA).**

1.1. Primero, calcular el valor de los activos con nivel de riesgo detallado ALTO y MODERADO en términos financieros Directos, Indirectos y Costos.

Se utilizan las siguientes categorías como referencia para estimar el costo total para cada activo, en donde aplique:

- **Valores Directos:**
  - Valor físico
  - Valor para la empresa
  - Valor para los usuarios
  - Propiedad intelectual
  - Otros valores
- **Valores Indirectos:**
  - Mejora de la productividad
  - Valor para la competencia
  - Valoración del mercado
  - Marca
  - Otros valores
- **Costos:**
  - Compra
  - Instalación
  - Implementación
  - Customización
  - Otros costos
- **Otros:**
  - Otros valores

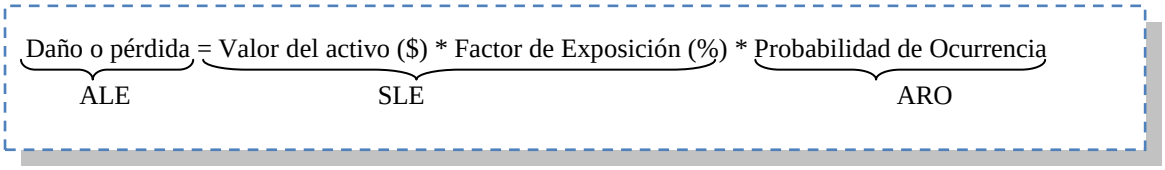
1.2. Después de cuantificar los activos en cada categoría, se calcula el valor total del activo es el siguiente:

Valor total del activo = Valores Directos + Valores Indirectos - Costos

1.3. Luego de haber obtenido los valores de cada uno de los activos, hacer una sumatoria por tipo de activo según el Impacto al Negocio previamente asignado *(cuadro 4-04)*. La empresa aplica un enfoque conservador al seleccionar el valor de activo mínimo en cada clase de Impacto al Negocio. Este enfoque simplifica la tarea de asignar valores monetarios a cada activo ya que se emplean las clases de activos.

El resultado es una lista de activos con prioridades y una estimación aproximada de su valor monetario.

2. **Determinar el impacto financiero inmediato de la pérdida del activo:** El impacto financiero de la pérdida del activo se ve marcado por la siguiente fórmula:



Para lo cual es necesario:

2.1. **Determinar el valor de expectativa de pérdida simple - SLE:** El SLE representa el importe total de los ingresos que se perderán si el riesgo se produce una vez. El factor de exposición (4-12) se multiplica por el valor del activo (VA) para generar la estimación cuantitativa de los impactos.

2.2. **Determinar la probabilidad de ocurrencia anual - ARO:** La probabilidad de ocurrencia de la amenaza es calculada en función del número de veces que la amenaza puede ocurrir en un período de tiempo. En el presente trabajo el período de tiempo es tres (3) años. Esta estimación después se convierte en una estimación anual. Por ejemplo, si se piensa que un riesgo se puede producir dos veces al año, la frecuencia anual es dos. Si un riesgo se puede producir una vez cada tres años, la frecuencia anual es un tercio, 33% o 0,33. Como ayuda para estimar la probabilidad, utilizar la siguiente guía para identificar y comunicar el valor cuantitativo con el fin de determinar la frecuencia anual.

Calificación Cualitativa	Descripción	Rango ARO	Ejemplos
Alta	Muy Probable	>= 1	Impacto de una vez o más por año
Media	Probable	.99 to .33	Al menos uno entre 1-3 años
Baja	No probable	< .33	Frecuencia de más de 3 años

Cuadro 4-17 Determinación de la Frecuencia Anual - ARO [1]

2.3. **Determinar la expectativa de pérdida anual - ALE:** La expectativa de pérdida anual proporciona un valor con el que la empresa puede presupuestar cuánto costará establecer controles o protecciones para prevenir este tipo de daño y brindar un nivel adecuado de protección. Para concluir la ecuación cuantitativa, multiplicar la frecuencia anual por la expectativa de pérdida simple.

3. **Determinación del costo de los controles:** Las pérdidas en una empresa se reducen implementando controles, por lo que el estándar ISO/IEC 27001 aporta confianza en este sentido, ya que la implementación de un Sistema de Gestión en Seguridad de la Información (SGSI) y Controles de Seguridad (Anexo A de la norma) asegura una importante reducción y eliminación de incidentes de seguridad; y al estar dentro de un ciclo de mejora continua, el sistema de gestión responde a las nuevas necesidades de seguridad de la empresa. Determinar el costo de los controles requiere estimaciones precisas de cuánto costará adquirir, probar, implementar, poner en funcionamiento y mantener el control o la solución propuesta, que para el propósito de la presente Tesis los controles se definen en función de la aplicación del estándar ISO/IEC 27001:2005[J]. Dichos costos deben incluir la compra, la implementación y configuración de la solución, el mantenimiento, la notificación de nuevas directivas o procedimientos, los cursos para usuarios y personal de TI acerca de cómo utilizar y dar soporte, supervisarlo y combatir la pérdida de comodidad o productividad que pueda imponer.

   Los expertos en seguridad de información y los administradores del sistema normalmente proponen controles con el fin de mitigar los riesgos encontrados y el costo aproximado de cada control.

Luego de una evaluación de riesgos la alta gerencia debe tomar una decisión sobre la gestión de los riesgos detectados, apoyado del Análisis Costo Beneficio. Algunas alternativas son[E] :

- **Asumir los riesgos sin hacer nada:** Esta alternativa es lógica únicamente cuando el perjuicio esperado no tiene valor alguno o cuando el costo de aplicación de medidas superaría al de la reparación del daño. En otras palabras, la organización conoce el riesgo y decide asumirlo sin tomar ninguna acción al respecto, bien porque no tiene capacidad o bien porque el coste para mitigar el riesgo es desproporcionado para los beneficios que aporta.
- **Aplicar medidas para mitigarlo:** mediante el diseño y la implantación de controles o medidas preventivas o que atenúen los impactos y las consecuencias del mismo. Para el caso de la presente Tesis, la medida propuesta es la aplicación del estándar ISO/IEC 27001:2005[J].

- **Transferirlo**: como por ejemplo contratar a una aseguradora de forma que si el riesgo se materializa exista una compensación externa que lo mitigue.

- **Evitar el riesgo:** mediante la eliminación del mismo (por ejemplo a través de la reingeniería de procesos o incluso suspendiendo la actividad que origina el riesgo sin penalizar los objetivos de negocio de la organización).

Las distintas opciones para hacer frente a los riesgos pueden ser utilizadas conjuntamente, si bien es destacable que no todos los riesgos pueden ser reducidos o prevenidos a un nivel aceptable. La continuidad de negocio constituye por sí misma una estrategia o una opción de respuesta para hacer frente a aquellos riesgos que pueden interrumpir las operaciones de la organización.

[E] Inteco – Deloitte, *Guía para PYMES, Cómo Implantar un Plan de Continuidad del Negocio*, 2010, página 40.

4.5. Evaluación Costo Beneficio

El objetivo del costo beneficio es el de proporcionar una medida de rentabilidad a un proyecto, mediante la comparación de los costos con los beneficios logrados en la realización del mismo. Los resultados se presentan a los directivos para que los tengan en cuenta en una etapa de toma de decisiones.

Para inversiones en seguridad, el ROSI[17] - Retorno de la Inversión en Seguridad (Return Of Security Investment) mide la relación entre el retorno que produce una inversión y la inversión propiamente dicha.

ROSI es un indicador financiero derivado del ROI (Return of Investment) utilizado para justificar la inversión en seguridad de la información en términos monetarios. El ROSI es un valor porcentual que relaciona el retorno o beneficio neto (costos ahorrados como consecuencia de evitar incidentes de seguridad o de mitigar los efectos de los mismos en caso de ocurrencia) con la inversión que produce dicho retorno.

Para calcular el ROSI de implementar la ISO/IEC 27001:2005, primero hay que determinar los valores de las pérdidas actuales y los costos de la aplicación la medida de seguridad mencionada. Una fórmula sencilla para el cálculo del ROSI propuesta por la Guía de Administración de Riesgos de Seguridad de Microsoft[1] es la siguiente:

$$ROSI\ (\%) = \frac{BENEFICIO\ (\$) - COSTO\ (\$)}{COSTO\ (\$)}$$

Donde, el BENEFICIO = Expectativa de Pérdida Anual antes de la aplicación de las medidas de seguridad - Expectativa de Pérdida Anual después de la aplicación de las medidas de seguridad. Lo que equivale a:

$$ROSI = \frac{[(ALE\ antes\ de\ controles - ALE\ después\ de\ controles) - Costo\ de\ los\ controles}{Costo\ de\ los\ controles}$$

Para que un proyecto sea en principio aceptable, ROSI debe ser positivo, lo que ocurre cuando el beneficio es mayor que el costo.

CAPÍTULO V: VISION GENERAL DE LA SEGURIDAD DE LA INFORMACIÓN EN LA EMPRESA SELECCIONADA

El presente capítulo corresponde a la primera fase hacia el análisis Costo Beneficio ya que se proporciona una visión general de la trayectoria, información estratégica y negocio de la empresa seleccionada, se analizan las generalidades del nivel de Seguridad de la Información en la misma para así contar con el conocimiento necesario sobre la empresa para luego en la segunda fase identificar los activos de información que ésta posee y la historia reciente de incidentes de seguridad que la empresa ha sufrido.

5.1. Historia de la empresa

"En 1963, un grupo de empresarios ecuatorianos asumieron el reto de entregarle al país una industria del acero, que en forma técnica y económica, cubriera las necesidades del sector de la construcción y afines. Desde su creación, ACERÍA DEL ECUADOR C.A. ADELCA ha mantenido una permanente innovación en sus sistemas de producción y en los servicios prestados a sus clientes, siendo necesario reinvertir sus beneficios, con la finalidad de dotarle a la empresa de una tecnología avanzada y personal capacitado." [16]

5.2. Información estratégica de la empresa

Misión: Líderes en el reciclaje para la producción de acero, con excelencia en el servicio, calidad, tecnología, sistemas de gestión, recursos humanos, seguridad industrial, protección ambiental y responsabilidad social.

Visión: Siempre pensando en el CLIENTE, con el mejor servicio y los mejores productos de acero.

Valores: El cliente es lo primero. Compromiso con la calidad y la productividad. Mejoramiento continuo. Trabajo en equipo.

[16] Sitio web de Adelca – Acería del Ecuador, Historia, 2011, Internet. http://www.adelca.com/sitio/esp/corporativo.php Acceso: marzo 2012

Estructura general de la empresa: La estructura organizacional de la empresa se presenta en el siguiente gráfico, donde puede apreciarse su estructura jerárquica establecida para la operación de la organización.

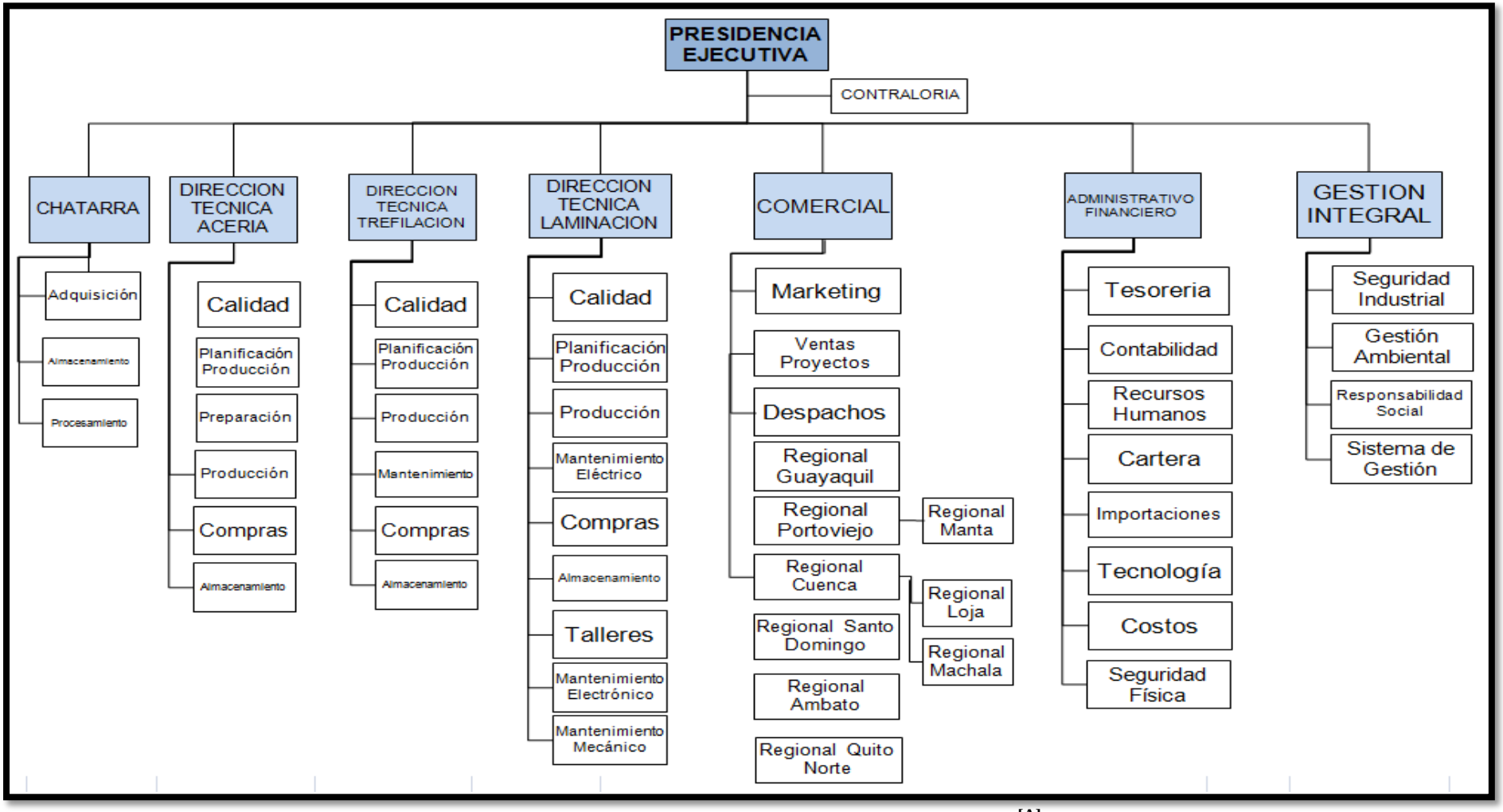


Figura 5-01 Estructura Organizacional de ADELCA[A]

5.3. Descripción del negocio y sector empresarial

ADELCA es una empresa del sector industrial ecuatoriano, ubicada en la provincia de Pichincha, dedicada al reciclaje de acero para la producción de materiales de construcción, manteniendo liderazgo en la Sierra y Oriente, su nivel de participación del mercado es del 35%. Cuenta con un total aproximado de 1200 empleados directos a nivel nacional, distribuidos entre personal de planta y obreros.

Sus clientes se distribuyen de la siguiente manera:

- Distribuidores/Subdistribuidores: 400
- Proyectos: 10
- Consumidores Finales: 50

Su cobertura se encuentra en:

- Fábrica en Alóag
- Guayaquil
- Cuenca
- Portoviejo
- Quito Norte
- Santo Domingo
- Ambato
- Loja
- Machala
- Manta

Unidades de Producción: Cuenta con tres unidades de producción: Acería, Laminación y Trefilación.[16]

- **Acería:** Procesa chatarra y entrega palanquillas (barras que son la Materia Prima para el proceso de laminación)

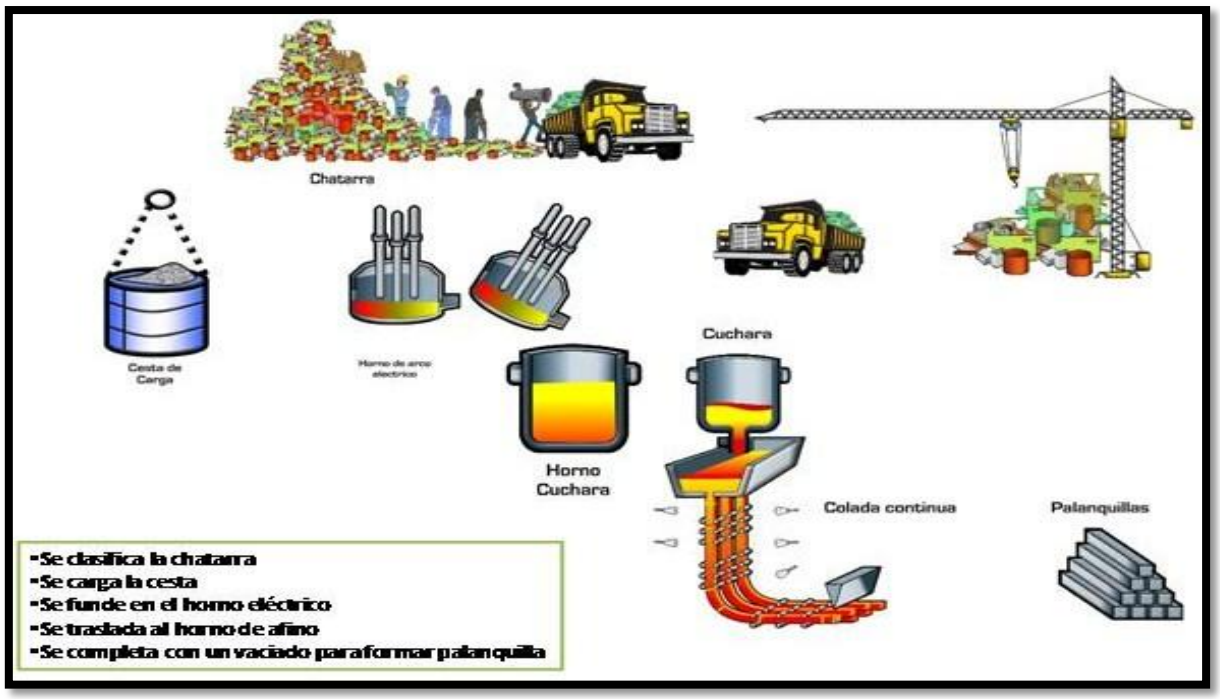


Figura 5-02 Proceso de Palanquillas[16]

- **Laminación:** Utiliza las barras de palanquilla y produce a altas temperaturas: varillas, perfiles y pletinas, en varias medidas.

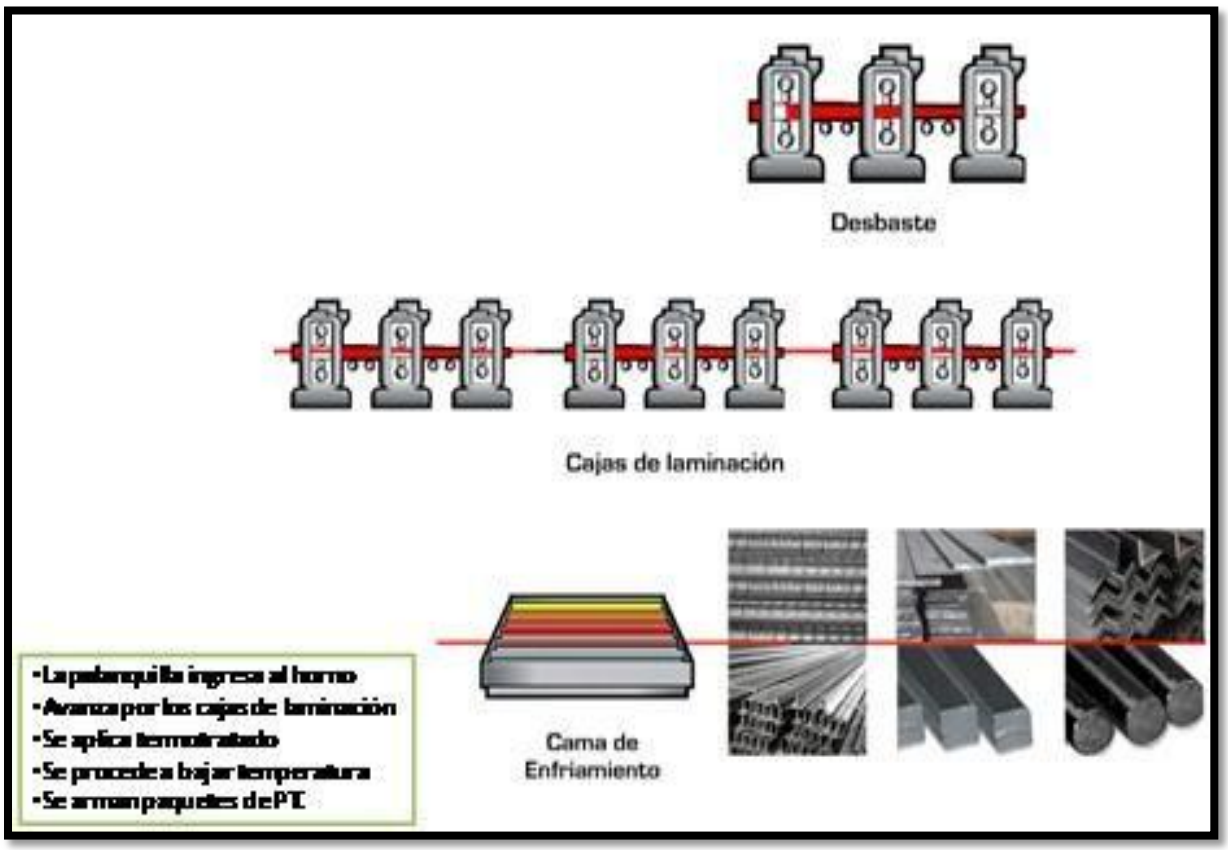


Figura 5-03 Proceso de Laminación[16]

- **Trefilación:** Es una unidad independiente. Su materia prima es el alambrón (rollos de alambre muy gruesos). Este material es importado. Esta unidad procesa en frío, mediante estiramiento y produce las siguientes familias de productos:
    - Varilla trefilada
    - Alambres (de púas, galvanizado, de construcción)
    - Clavos

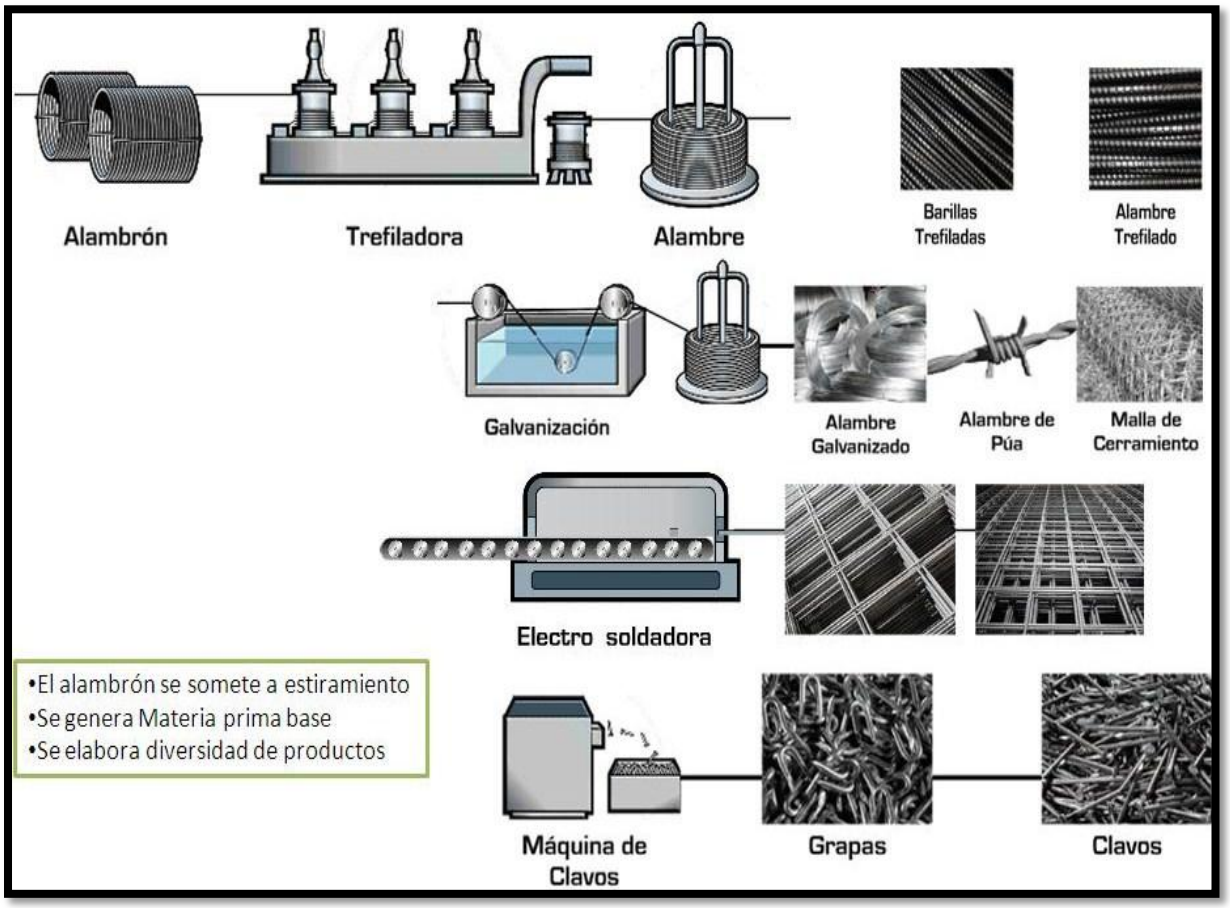


Figura 5-04 Proceso de Trefilación[16]

Crecimiento del Negocio: A continuación se presenta un resumen del crecimiento de la empresa en los últimos diez años:

Tema	Año 2001	Año 2011	% Crecimiento
Sector de la empresa	Manufactura	Reciclaje/ manufactura	
Número de empleados	650	1200	84.62%
Número de Sucursales	1	9	800%
Volumen de Vtas. TM.	120000 anuales	240000 anuales	100%
Materia Prima	Importada	Proceso local de chatarra	
Centro acopio Chatarra	0	5	500%
Número de plantas	2	3	50%
Certificaciones	INEN	INEN – ISO 9000 – ISO 14001 – OSHAS 18001	
Número de Usuarios de red	75	250	233.33%
Personal de Tecnología	2	4	100%
Sistemas Informáticas	Aplicaciones propias	ERP- Qlikview – Evolution	
Internet	No	Si	5 MB
Correo Electrónico	No	Si	250 usrs.
Telefonía	Convencional	IP	

Cuadro 5-01 Crecimiento de la empresa en los últimos 10 años[A]

Aspectos a considerar:

- La empresa ha cambiado su estrategia de producción, de ser un importador a un reciclador de chatarra para producir materia prima para su negocio.
- La empresa ha experimentado en los últimos diez años un crecimiento muy importante en muchos aspectos de su negocio: Número de empleados, volumen de ventas, número de sucursales. Los records en ventas en la historia del negocio se han presentado en los años 2008 al 2011.
- En lo referente a usuarios de información su crecimiento del 233.33%, nos muestra como la organización ha ido requiriendo del apoyo tecnológico para su gestión.

- En cuanto a certificaciones la empresa ha obtenido durante este tiempo las siguientes: ISO 9001, ISO14001 y OHSAS 18001.
- De igual forma el área de tecnología ha experimentado un crecimiento del 100% durante este período.
- Con respecto al desarrollo de sistemas informáticos en casa, se cambió a la compra de licencias de software orientado para la industria y que permita un manejo integral. Se adquirió BaaN, software tipo ERP, actualmente de la empresa americana INFOR. Para el área de recursos humanos se adquirió Evolution, software ecuatoriano de la empresa EBS.
- En cuanto a Internet, se pasó de la utilización de líneas dial up a contar con dos salidas, una en planta con mayor ancho de banda y otra en Cumbaya de menor salida.
- Respecto al correo electrónico, de cuentas específicas para usuarios claves, se ha remplazado la solución de IBM, Lotus Notes por la de Microsoft Exchange con una solución empresarial que atiende a más de 250 usuarios.
- En lo referente a Telefonía, de centrales analógicas se ha cambiado a centrales IP, integradas en algunos puntos con la red de datos.

En términos generales se refleja un crecimiento importante de la empresa en todos los aspectos durante los últimos diez años.

5.4. Situación actual de la seguridad de la información en la empresa

Para tener una base de partida respecto a la seguridad de la información en la empresa, se ha procedido a comparar su situación con los resultados principales de la encuesta:

5.4.1. Comparativo respecto a la III Encuesta latinoamericana de Seguridad de Información

- **Presupuesto para Seguridad de la información:**

  Para el año 2011 la empresa invirtió menos de 50.000 dólares en este tema, lo cual le ubica en el mismo nivel que el promedio de empresas de la encuesta. *Para el resultado de este tema en la encuesta, dirigirse a*

  Presupuestos *en el capítulo II, página 15 del presente documento.*

- **Incidentes de seguridad:**

  Los mayores promedios en la encuesta demuestran que la instalación de software no autorizado y los virus ocupan el mayor porcentaje, para la empresa la mayor cantidad de fallas han estado en Virus y fraudes. *Para el resultado de este tema en de la encuesta, dirigirse a*

  Incidentes de Seguridad *en el capítulo II, página 15 del presente documento.*

- **Notificación de Incidentes:**

  En la encuesta se muestra que el nivel directivo es el mayor notificador de incidentes, además del equipo de atención de incidentes y un alto porcentaje no se denuncia. Para la empresa la mayor cantidad proviene de grupos de manejo de incidentes, sin existir un involucramiento del nivel ejecutivo. *Para el resultado de este tema en de la encuesta, dirigirse a Notificación de Incidentes de Seguridad en el capítulo II, página 16 del presente documento.*

- **Política de Seguridad de la información:**

  La encuesta marca una tendencia hacia disponer de una política formal, escrita, documentada e informada a la organización, la empresa dispone de una política que no ha pasado de su etapa de desarrollo. *Para el resultado de este tema en de la encuesta, dirigirse a Políticas de Seguridad de la Información en el capítulo II, página 17 del presente documento.*

- **Obstáculos para implementar la Seguridad de la Información:**

  Entre los principales de acuerdo a la encuesta, están la falta de colaboración entre áreas, poco entendimiento de la Seguridad de la Información, y falta de apoyo directivo, circunstancias que son similares dentro de la organización. *Para el resultado de este tema en de la encuesta, dirigirse a*

  Obstáculos para implementar la seguridad *en el capítulo II, página 17 del presente documento.*

- **Estándares y buenas prácticas**

  La encuesta presenta entre los principales utilizados a: ISO/IEC 27001[J] e ITIL, la empresa no cuenta con ninguna práctica de los estándares descritos. *Para el resultado de*

este tema en de la encuesta, dirigirse a 2.5. Evaluación de estándares de seguridad de en el capítulo II, página 28 del presente documento.

En resumen, la empresa al ser comparada con los resultados en otros países Latinoamericanos, muestra un patrón de comportamiento muy similar y en algunos casos hasta menor, a los resultados obtenidos. El estándar ISO/IEC 27001[J], más difundido en otros países, en Ecuador constituye una práctica de seguridad poco utilizada. Esto abre una oportunidad interesante para su consideración y evaluación dentro de este proyecto.

A continuación se presentan aspectos generales de la empresa relacionados con la seguridad de la información en la organización, a considerar:

- La empresa cuenta con certificaciones ISO 9001, ISO14001 y OHSAS 18001, pero no cuenta con un Sistema de Gestión de la Seguridad de la información (SGSI), formal y documentado, por el escaso conocimiento de su alcance y beneficios.
- La empresa no cuenta con ningún estándar para garantizar la seguridad de la información. Se ha utilizado el criterio común como práctica para la generación de políticas y procedimientos.
- La empresa no cuenta con una política de seguridad de la información, existe una realizada en el año 2009 que no ha sido difundida, lo cual incide en que la información crítica y los activos de información de la compañía no cuentan con la seguridad adecuada.
- No se dispone de una metodología formal para la identificación de riesgos de Seguridad de Información, los análisis realizados han sido efectuados en su mayoría con la aplicación de criterios comunes.
- No existe un presupuesto definido para invertir en seguridad de la información, se hace una inversión en función de las necesidades presentadas.
- Las principales fallas en la seguridad de la información en la empresa se han presentado por: alteración de datos y fraudes. Lo cual ha puesto en riesgo la estabilidad de la empresa.
- La empresa no cuenta con un plan corporativo de capacitación y entrenamiento, lo cual hace que también en los temas relacionados con la seguridad de la información, sea encontrada similar deficiencia.

- La función de seguridad de la información en la empresa no está considerada como una tarea principal, con personal dedicado en su totalidad a esta función. Las actividades de administración de seguridad son algunas de las funciones a cargo de una sola persona que es el Administrador de Redes y Comunicaciones. La seguridad física, está bajo responsabilidad del área de Seguridad de la empresa, incluyéndose todo lo relacionado a equipo de cómputo.

Como se puede observar, la empresa no ha considerado a la Seguridad de la Información como objetivo de prioridad, a pesar del crecimiento experimentando y la existencia de activos de información que se deben proteger.

CAPÍTULO VI: ANÁLISIS COSTO BENEFICIO DE LA APLICACIÓN DEL ESTÁNDAR ISO/IEC 27001:2005 A LA EMPRESA INDUSTRIAL SELECCIONADA

El presente capítulo representa al tema medular del presente trabajo de Tesis, en el cual se seguirán los lineamientos para el cálculo de Costo Beneficio establecidos en el Capítulo IV. En este capítulo se proporciona en detalle la Recopilación de información sobre los activos de información de la empresa, la Evaluación de Riesgos que propone la Guía de Administración de Riesgos de Seguridad de Microsoft[1] y finalmente el análisis Costo Beneficio a través de ROSI[31].

Para mayor entendimiento, se seguirá el procedimiento tomando como base la metodología propuesta, para dos activos de información. Los resultados globales se encuentran en Anexos adjuntos al presente documento.

6.1. Recopilación de información sobre activos de la información de la empresa

En este punto se expone el resultado del levantamiento de información de los activos de información más relevantes para la empresa, según la Guía de Administración de Riesgos de Seguridad de Microsoft[1] y los pasos descritos en el capítulo IV, punto "4.3. Recopilación de Datos sobre activos de la información de la empresa".

1. **Realizar la descripción de los activos:** Los activos definidos por los usuarios claves para la empresa son 78, cada uno de los cuales lleva la siguiente nomenclatura:

No. Activo = AIn.x

[31] ROSI: Return of Security Investment o Retorno de la Inversión en Seguridad

En donde,

- **AI** = Activo de Información
- **n** = Número secuencial del activo
- **x** = Número secuencial para el Nivel de Defensa *(a partir del punto 4)*

El desarrollo de la metodología se realizará para los activos de información descritos en el cuadro a continuación:

No. Activo	Descripción de los activos de información de la empresa		
	Nombre de Activo	Localización del activo	Propietario responsable
AI1.	**Microsoft Active Directory®**	Planta	Tecnología
AI25.	**Datos de clientes y créditos**	Planta y Sucursal	Cartera

Cuadro 6-01 Descripción de activos de información que se utilizarán como referencia[A]

2. **Asignar la clase de activo de información:** Cada uno de los activos determinados ha sido asociado a una Clase de Activo y un Entorno Global de Tecnología de Información en base a lo descrito en el punto 4.3 (Cuadro 4-02 Clasificación de activos). *Este nivel de clasificación para todos los activos se muestra en el Anexo C del presente documento.*

La Clase de Activo y el Entorno Global de Tecnología para los activos de referencia es el siguiente:

No. Activo	Clasificación de los activos *(cuadro 4-02)*		
	Nombre de Activo *(cuadro 6-01)*	Clase de Activo	Entorno Global de TI
AI1.	Microsoft Active Directory®	**Servicios de TI**	**Infraestructura básica**
AI25.	Datos de clientes y créditos	**Tangible**	**Datos de intranet**

Cuadro 6-02 Clasificación de activos[A]

3. **Identificar incidentes de seguridad relacionados a cada uno de los activos de información:** Los incidentes a lo largo de la historia reciente de esta empresa representan alrededor de 2 millones de dólares en pérdidas, pudiendo evitarse esta alta cantidad de pérdidas monetarias con la implementación de controles de seguridad más rígidos y ajustado a las necesidades de la empresa.

   En el siguiente cuadro se muestra que para el primer activo de referencia AI1., no se han identificado incidentes directamente relacionados y para el segundo activo de referencia AI25, se describe el incidente suscitado en la empresa, junto con el costo que éste causó:

   Para un detalle de todos los incidentes relacionados con los activos de información recopilados, referirse al Anexo C del presente documento.

No. Activo	Descripción de los activos *(cuadro 6-01)*	Clasificación de los activos *(cuadro 6-02)*		Incidentes de seguridad	
	Nombre de Activo	Clase de Activo	Entorno Global de TI	Descripción del Incidente relacionado directamente con el activo	Costo USD
AI1.	Microsoft Active Directory®	Servicios de TI	Infraestructura básica	No se han registrado incidentes que afecten directamente a este activo.	-
AI25.	Datos de clientes y créditos	Tangible	Datos de intranet	La empresa detectó en enero del 2011 un fraude en el área de Cobranzas, donde aprovechándose de una vulnerabilidad en el sistema ERP y de deficiencias en el control interno en el proceso de registro de ingresos, se venían alterando desde el año 2009 los saldos de un grupo de clientes, con el objetivo de mantener el estado de su cartera en valores por vencer. Esto provocó un riesgo para la empresa de $950.000.	950.000
				En la Sucursal de Guayaquil, se detectó una compra con cheque robado Responsable: Asistente de Cartera.	32.000
				En la Sucursal de Guayaquil la jefa administrativa, recibía dineros de clientes y realizaba mala utilización.	10.000
				En la Sucursal Sto Domingo, se detectó una mala utilización de pagos de clientes.	60.000
				En Portoviejo, se detectó una mala utilización de pagos de clientes.	12.000
				En la fábrica, se detectó una compra con cheque certificado falsificado.	42.000
				Valores incobrables que maneja la empresa.	60.000

Cuadro 6-03 Identificación de incidentes de los Activos de la Información referencia[A]

El detalle de los incidentes por activo de información mostrados en el Anexo C del presente documento, muestra el registro de incidentes graves, como la identificación de un fraude financiero, ocasionado por el aprovechamiento de vulnerabilidades en el sistema principal de la empresa.

4. **Establecer niveles de defensa de los activos:** Cada activo puede ser evaluado en varios niveles de defensa *(cuadro 4-03, capítulo IV)*. Para el caso de los activos de referencia, los niveles de defensa evaluados son los siguientes:

   - **AI.1. Directorio Activo:** El Directorio activo dispone de un nivel de defensa a nivel de host (3), por tratarse de un servidor principal.

   - **AI.25.1. Datos de clientes y créditos:** Los datos de clientes y créditos disponen de los niveles de defensa host (3) y datos (5) por tratarse de *datos* almacenados en un *servidor*.

   El siguiente cuadro resume el Nivel de Defensa para los activos de referencia.

No. Activo	Nombre de Activo *(cuadros 6-01, 6-02 y 6-03)*	Nivel de defensa *(cuadro 4-03)*	
AI1.1	Microsoft Active Directory®	3	Host
AI1.25.1	Datos de clientes y créditos	3	Host
AI1.25.2		5	Datos

Cuadro 6-04 Niveles de Defensa de los activos de referencia[A]

La información de los niveles de defensa de todos los activos se encuentra disponible en el Anexo D del presente documento.

5. **Definir el Nivel de Impacto del activo para el negocio:** Cada activo tiene un nivel de impacto respecto al negocio, el mismo que puede ser alto, medio o bajo *(cuadro 4-04, capítulo IV).* Para el caso de los activos de referencia los niveles de impacto son los siguientes:

- **AI.1. Directorio Activo:** ***Nivel de defensa Host (3); Impacto al Negocio ALTO (10):*** Este activo es de alto impacto para el negocio, ya que un problema a nivel de servidor principal, puede ocasionar que la empresa no disponga de acceso a varios de sus servicios principales, como el caso del correo electrónico y el acceso a los sistemas claves del negocio, lo cual puede generar pérdidas importantes para la empresa.

- **AI.25.1. Datos de clientes y créditos:** ***Nivel de defensa Host (3), Impacto al Negocio ALTO (10):*** Este activo es de alto impacto para el negocio, ya que un problema a nivel de servidor principal, puede ocasionar que la empresa no disponga de acceso al sistema BaaN-ERP, lo cual puede generar pérdidas importantes para la empresa ya que almacena los datos de clientes y créditos.

- **AI.25.1. Datos de clientes y créditos:** ***Nivel de defensa Datos (5), Impacto al Negocio ALTO (10):*** Este activo es de alto impacto para el negocio, ya que un problema a nivel de sus datos, puede ocasionar que la empresa realice aprobaciones inadecuadas de créditos y se de apertura para fraudes, lo cual puede generar pérdidas importantes para la empresa.

El siguiente cuadro resume el Nivel de Impacto al Negocio para los activos de referencia.

No. Activo	Nombre de Activo *(cuadros 6-01, 6-02 y 6-03)*	Nivel de defensa *(cuadro 6-04)*	Nivel de Impacto al Negocio *(cuadro 4-04)*
AI1.1	Microsoft Active Directory®	3	**10**
AI1.25.1	Datos de clientes y créditos	3	**10**
AI1.25.2		5	**10**

Cuadro 6-05 Niveles de Impacto al Negocio de los activos de referencia[A]

La información del nivel de impacto al Negocio de todos los activos se encuentra disponible en el Anexo D del presente documento.

6. **Establecer Amenazas de seguridad:** Las amenazas establecidas para los activos de referencia y sus niveles de defensa son las siguientes:

- **AI.1. Directorio Activo:** ***Nivel de defensa Host (3):*** La principal amenaza en este activo está dada por las posibles fallas que afectarían la disponibilidad de los servicios y accesos a los diferentes ambientes.

- **AI.25.1. Datos de clientes y créditos:** ***Nivel de defensa Host (3):*** La principal amenaza bajo el nivel de defensa de host en este activo está dada por las posibles caídas de servicios que afectan la disponibilidad de información de los clientes.

- **AI.25.1. Datos de clientes y créditos:** ***Nivel de defensa Datos (5):*** Respecto a este nivel de defensa, la amenaza está relacionada con que el cliente ante problemas con crédito decida buscar otro proveedor.

El siguiente cuadro resume las amenazas para los activos de referencia.

No. Activo	Nivel de Defensa *(cuadro 6-04)*	Impacto al Negocio *(cuadro 6-05)*	Descripción de la amenaza
AI1.1	3	10	**Falla en el servidor puede afectar el acceso a los distintos ambientes y crear indisponibilidad en los servicios**
AI24.1	5	10	**Cliente puede encontrar otros Proveedores que cumplan sus necesidades de información**
AI25.1	3	10	**Caída de servicios Se pone en riesgo la disponibilidad de la información, necesaria e indispensable para trabajar con clientes.**

Cuadro 6-06 Amenazas de los activos de referencia[A]

La información de las amenazas de todos los activos se encuentra disponible en el Anexo D del presente documento.

7. Definir Vulnerabilidades:

Las vulnerabilidades establecidas para los activos de referencia y sus niveles de defensa son las siguientes:

- **AI.1. Directorio Activo:** ***Nivel de defensa Host (3):*** La principal vulnerabilidad en este activo es la falta de un equipo de respaldo que permita restablecer los servicios y el acceso a los diferentes ambientes.

- **AI.25.1. Datos de clientes y créditos:** ***Nivel de defensa Host (3)****:* La principal vulnerabilidad en este activo es la falta de un equipo de respaldo que permita restablecer los servicios de producción, con la agilidad que el negocio requiere.

- **AI.25.1. Datos de clientes y créditos:** ***Nivel de defensa Datos (5):*** Respecto a este nivel de defensa, la vulnerabilidad está dada por la falta de políticas y procedimientos actualizados para el control de créditos de clientes.

El siguiente cuadro resume las vulnerabilidades para los activos de referencia.

No. Activo	Nivel de Defensa *(cuadro 6-04)*	Impacto al Negocio *(cuadro 6-05)*	Descripción de la amenaza *(cuadro 6-06)*	Descripción de la vulnerabilidad
AI1.1	3	10	Falla en el servidor puede afectar el acceso a los distintos ambientes y crear indisponibilidad en los servicios	**No se dispone de un equipo de respaldo**
AI25.1	3	10	Caída de servicios Se pone en riesgo la disponibilidad de la información, necesaria e indispensable para trabajar con clientes.	**No se dispone de un equipo y ambiente de respaldo**

No. Activo	Nivel de Defensa *(cuadro 6-04)*	Impacto al Negocio *(cuadro 6-05)*	Descripción de la amenaza *(cuadro 6-06)*	Descripción de la vulnerabilidad
AI25.2	5	10	Fallas por alteraciones de datos y fraudes aprovechando brechas en la seguridad de la información afectan la disponibilidad e integridad de la información.	**No se disponen de políticas y procedimientos actualizados para el control de créditos que eviten el uso inadecuado de datos que ponen en riesgo el prestigio de la empresa**

Cuadro 6-07 Vulnerabilidades de los activos de referencia[A]

La información de las vulnerabilidades de todos los activos se encuentra disponible en el Anexo D del presente documento.

8. **Identificar el Nivel de exposición:** La estimación de los daños posibles para los activos de referencia se presenta a continuación:

- **AI.1. Directorio Activo:** ***Nivel de defensa Host (3):*** El nivel de exposición para este activo se considerada MODERADO, por cuanto un daño en el servidor tiene su impacto pero no se puede considerar una pérdida total.

- **AI.25.1. Datos de clientes y créditos:** *Nivel de defensa Host (3):* El nivel de exposición para el servidor de los datos se encuentra en BAJA, por cuanto una pérdida del servidor por los niveles de redundancia en algunos de sus elementos hace que esta probabilidad sea mínima.

- **AI.25.1. Datos de clientes y créditos:** *Nivel de defensa Datos (5):* Para el caso de los datos el nivel de exposición es ALTO, por cuanto un daño en su información no puede dejar rastro para ser reconstruida o recuperada.

El siguiente cuadro resume el nivel de exposición para los activos de referencia.

No. Activo	Nivel de Defensa *(cuadro 6-04)*	Impacto al Negocio *(cuadro 6-05)*	Descripción de la amenaza *(cuadro 6-06)*	Descripción de la vulnerabilidad *(cuadro 6-07)*	Nivel de Exposición *(cuadro 4-05)*
AI1.1	3	10	Falla en el servidor puede afectar el acceso a los distintos ambientes y crear indisponibilidad en los servicios	No se dispone de un equipo de respaldo	**Moderada**
AI25.1	3	10	Caída de servicios Se pone en riesgo la disponibilidad de la información, necesaria e indispensable para trabajar con clientes.	No se dispone de un equipo y ambiente de respaldo	**Baja**
AI25.2	5	10	Fallas por alteraciones de datos y fraudes aprovechando brechas en la seguridad de la información afectan la disponibilidad e integridad de la información.	No se disponen de políticas y procedimientos actualizados para el control de créditos que eviten el uso inadecuado de datos que ponen en riesgo el prestigio de la empresa	**Alta**

Cuadro 6-08 Nivel de exposición de los activos de referencia[A]

La información del nivel de exposición de todos los activos se encuentra disponible en el Anexo D del presente documento.

6.2. Evaluación de Riesgos Cualitativa

En esta fase se seguirán los pasos descritos en el punto 4.4.1. (capítulo IV). El resultado será un listado resumido de prioridades de riesgo sobre los activos identificados en el punto 6.1.

1. **Determinar el impacto:** El impacto medido en función del nivel de exposición y el impacto al negocio, presenta los siguientes resultados:

- **AI.1. Directorio Activo:** ***Nivel de defensa Host (3):*** Para este activo la empresa estima que existe un nivel de exposición MODERADO a que una falla en el servidor afecte el acceso a los distintos ambientes y cree indisponibilidad (amenaza) en el servicio de Active Directory (activo) al no disponer de un equipo de respaldo en el cual se pueda cargar la información (vulnerabilidad). Con esta premisa se obtienen las siguientes entradas para la matriz de Impacto (cuadro 6-09):

MATRIZ_IMPACTO [MODERADO, ALTO]=**Impacto ALTO**

		Impacto		
Clase de activo por Impacto al Negocio *(6-05)*	**10**	Impacto moderado	**Impacto alto**	Impacto alto
	5	Impacto bajo	Impacto moderado	Impacto alto
	2	Impacto bajo	Impacto bajo	Impacto moderado
		Bajo	**Moderado**	**Alto**
		Nivel de exposición *(6-08)*		

Cuadro 6-09 Impacto del activo de referencia AI1.1[1]

- **AI.25.1. Datos de clientes y créditos:** ***Nivel de defensa Host (3):*** Para este activo, la empresa estima que existe un nivel de exposición BAJO a que una falla en el servidor principal afecte el acceso a la información de clientes y cree indisponibilidad (amenaza) en el servicio de crédito (activo) al no disponer de un equipo de respaldo en el cual se pueda cargar la información (vulnerabilidad). Con esta premisa se obtienen las siguientes entradas en la matriz de Impacto *(cuadro 6-10)*:

MATRIZ_IMPACTO [BAJO, ALTO]=**Impacto MODERADO**

		Impacto		
Clase de activo por Impacto al Negocio *(6-05)*	**10**	**Impacto moderado**	Impacto alto	Impacto alto
	5	Impacto bajo	Impacto moderado	Impacto alto
	2	Impacto bajo	Impacto bajo	Impacto moderado
		Bajo	**Moderado**	**Alto**
		Nivel de exposición *(6-08)*		

Cuadro 6-10 Impacto del activo de referencia AI25.1[1]

- **AI.25.2. Datos de clientes y créditos:** ***Nivel de defensa Datos (5):*** Para este activo, la empresa estima que existe un nivel de exposición ALTO a que una falla en la información de clientes y crédito, cree desconfianza e indisponibilidad (amenaza) en el servicio de crédito de la empresa (activo) al no disponer de información y procedimientos adecuados que eviten el riesgo de perder ingresos de la empresa (vulnerabilidad). Con esta premisa se obtienen las siguientes entradas en la matriz de Impacto *(cuadro 6-11)*:

MATRIZ_IMPACTO [ALTO, ALTO]=**Impacto ALTO**

		Impacto		
Clase de activo por Impacto al Negocio *(6-05)*	**10**	Impacto moderado	Impacto alto	**Impacto alto**
	5	Impacto bajo	Impacto moderado	Impacto alto
	2	Impacto bajo	Impacto bajo	Impacto moderado
		Bajo	**Moderado**	**Alto**
		Nivel de exposición *(6-08)*		

Cuadro 6-11 Impacto del activo de referencia AI25.2[1]

La información del nivel de impacto resumido de todos los activos se encuentra disponible en el Anexo E del presente documento.

2. **Estimar la probabilidad del impacto:** Se define en función del tiempo estimado de ocurrencia del impacto.

   - **AI.1. Directorio Activo:** ***Nivel de defensa Host (3):*** La empresa estima que la probabilidad de que el impacto ocurra en la empresa es **MEDIA**, esperándose un impacto entre dos o tres años *(cuadro 4-07)*.

   - **AI.25.1 Datos de clientes y créditos:** ***Nivel de defensa Host (3):*** La empresa estima que la probabilidad de que el impacto ocurra en la empresa es **BAJA**, por cuanto no se espera que ocurra ningún impacto en tres años *(cuadro 4-07)*.

   - **AI.25.2 Datos de clientes y créditos:** ***Nivel de defensa Datos (5)****:* La empresa estima que la probabilidad de que el impacto ocurra en la empresa es **ALTA**, esperándose uno o varios impactos en un año *(cuadro 4-07)*.

   La información de la probabilidad de impacto de todos los activos se encuentra disponible en el Anexo E del presente documento.

3. **Asignar el nivel de riesgos:** Dado el impacto y probabilidad de ocurrencia determinada por la empresa, el nivel de riesgos para los activos de referencia es:

   - **AI.1. Directorio Activo:** ***Nivel de defensa Host (3):*** ALTO, según la matriz de Riesgo resumido *(cuadro 4-08)*:

MATRIZ_RIESGO [MEDIA, ALTO]= **Riesgo ALTO**

		Riesgo		
Impacto *(6-03)*	Alto	Riesgo moderado	**Riesgo alto**	Riesgo alto
	Moderado	Riesgo bajo	Riesgo moderado	Riesgo alto
	Bajo	Riesgo bajo	Riesgo bajo	Riesgo moderado
		Baja	**Media**	**Alta**
		Probabilidad del impacto ***(punto 2)***		

Cuadro 6-12 Nivel de riesgo resumido del activo de referencia AI1.1[1]

- **AI.25.1 Datos de clientes y créditos:** ***Nivel de defensa Host (3)****:* BAJO, según la matriz de Riesgo resumido *(cuadro 4-08)*:

  MATRIZ_RIESGO [BAJO, MODERADO]= **Riesgo BAJO**

		Riesgo		
Impacto *(6-03)*	Alto	Riesgo moderado	Riesgo alto	Riesgo alto
	Moderado	**Riesgo bajo**	Riesgo moderado	Riesgo alto
	Bajo	Riesgo bajo	Riesgo bajo	Riesgo moderado
		Baja	**Media**	**Alta**
		Probabilidad del impacto ***(punto 2)***		

Cuadro 6-13 Nivel de riesgo resumido del activo de referencia AI25.1[1]

- **AI.25.2 Datos de clientes y créditos:** *Nivel de defensa Datos:* ALTO, según la matriz de Riesgo resumido *(cuadro 4-08)*:

  MATRIZ_RIESGO [ALTO, ALTO]= **Riesgo ALTO**

		Riesgo		
Impacto *(6-03)*	Alto	Riesgo moderado	Riesgo alto	**Riesgo alto**
	Moderado	Riesgo bajo	Riesgo moderado	Riesgo alto
	Bajo	Riesgo bajo	Riesgo bajo	Riesgo moderado
		Baja	Media	Alta
		Probabilidad del impacto *(punto 2)*		

Cuadro 6-14 Nivel de riesgo resumido del activo de referencia AI25.2[1]

La lista resumida de riesgos de los activos analizados (AI1.1 – AI25.1 – AI25.2) está en el siguiente cuadro; y la lista resumida de riesgos del total de activos (78) identificados por la empresa, se encuentra en el Anexo E del presente documento.

No. Activo *(cuadros 6-01 y 6-02)*	Impacto *(cuadro 6-03)*	Probabilidad *(punto 2)*	Riesgo *(cuadros 6-12, 6-13 y 6-14)*
AI1.1	Alto	Medio	**Alto**
AI25.1	Moderado	Bajo	**Bajo**
AI25.2	Alto	Alto	**Alto**

Cuadro 6-15 Lista resumida de riesgos del activo de información utilizado como referencia[A]

4. **Selección de riesgos para el nivel detallado.** Se puede observar en el Anexo E que de los 78 activos identificados en la fase de Recopilación de información de activos de información de la empresa (6.1) (existen 106 registros ya que cada activo tiene más de un nivel de defensa), se determina que 34 activos tienen un nivel de riesgo ALTO, los cuales serán tomados en cuenta para la asignación de niveles de riesgo detallado.

   En el caso de los tres activos de referencia utilizados para mostrar los cálculos, pasan al nivel de detalle los activos por nivel de defensa cuyo nivel de riesgo está calificado como ALTO:

- AI.1 (**Directorio Activo:** *Nivel de defensa Host (3))* y
- AI.25.2 (**Datos de clientes y créditos:** *Nivel de defensa Datos (5))*.

El total de activos seleccionados para el nivel detallado se adjuntan en el siguiente detalle:

No. Activo	Clase de Activo *(cuadro 4-02)*	Entorno Global de TI *(cuadro 4-02)*	Nombre del Activo	Niveles de Defensa aplicables *(cuadro 4-03)*
AI1.1	Servicios de TI	Infraestructura básica	Microsoft Active Directory®	Host
AI5.1	Servicios de TI	Infraestructura básica	Almacenamiento de datos	Host
AI9.3	Servicios de TI	Infraestructura básica	Soporte a Usuarios	Datos
AI11.1	Servicios de TI	Infraestructura básica	Mantenimiento de Hardware Servidores	Host
AI12.2	Servicios de TI	Mensajería	Correo electrónico(Microsoft® Exchange)	Datos
AI16.1	Tangible	Datos de intranet	Software de aplicación BaaN ERP	Aplicación
AI18.2	Tangible	Datos de intranet	Software de oficina para usuario final	Aplicación
AI22.1	Tangible	Datos de intranet	Planes estratégicos	Datos
AI24.1	Tangible	Datos de intranet	Datos de pedidos de clientes	Datos
AI25.2	Tangible	Datos de intranet	Datos de clientes y créditos	Datos
AI26.2	Tangible	Datos de intranet	Datos de Facturación	Datos
AI28.2	Tangible	Datos de intranet	Datos de Inventarios de materia prima, producto terminado, repuestos	Datos
AI29.2	Tangible	Datos de intranet	Datos de Recursos Humanos y nómina	Host

No. Activo	Clase de Activo *(cuadro 4-02)*	Entorno Global de TI *(cuadro 4-02)*	Nombre del Activo	Niveles de Defensa aplicables *(cuadro 4-03)*
AI30.1	Tangible	Datos de intranet	Datos financieros	Host
AI35.2	Tangible	Datos de intranet	Información Gerencial	Datos
AI43.1	Tangible	Datos de intranet	Datos para pistas de auditoría	Datos
AI45.1	Tangible	Datos de extranet	Datos de pedidos a proveedores	Datos
AI47.1	Tangible	Infraestructura física	Servidores AIX	Host
AI48.1	Tangible	Infraestructura física	Servidores INTEL	Host
AI49.1	Tangible	Infraestructura física	Equipos de escritorio	Físico
AI51.1	Tangible	Infraestructura física	Impresoras	Físico
AI58.1	Tangible	Infraestructura física	Enlaces de datos e Internet	Red
AI61.1	Tangible	Infraestructura física	Respaldos de información (cintas, DVD, discos duros)	Físico
AI63.2	Tangible	Infraestructura física	Sistemas de control de accesos	Datos
AI64.1	Tangible	Infraestructura física	Fuentes de alimentación regulada	Host
AI65.1	Tangible	Infraestructura física	Sistemas de alimentación ininterrumpida (UPS)	Host
AI66.1	Tangible	Infraestructura física	Sistemas contra incendios	Host
AI67.1	Tangible	Infraestructura física	Sistemas de aire acondicionado	Host
AI70.1	Intangible	Personal	Productividad de empleados	Datos
AI71.1	Tangible	Personal	Usuarios	Datos

No. Activo	Clase de Activo *(cuadro 4-02)*	Entorno Global de TI *(cuadro 4-02)*	Nombre del Activo	Niveles de Defensa aplicables *(cuadro 4-03)*
AI72.1	Tangible	Personal Tecnología	Soporte	Datos
AI75.1	Intangible	Empresa	Reputación	Datos
AI77.1	Tangible	Datos de intranet	Datos Configuración BDD ERP	Datos
AI78.1	Tangible	Datos de intranet	Datos Configuración BDD Evolution	Datos

Cuadro 6-16 Lista de activos para nivel de riesgo detallado[A]

5. **Definición de controles de acuerdo a la norma ISO/IEC 27001:2005:** En base al Anexo A de la norma ISO/IEC 27001:2005, los controles establecidos para cada uno de los activos del nivel detallado se encuentran en el Anexo F-02.

   Para los activos de referencia se detallan a continuación:

No. Activo	Controles *(Anexo A de la ISO/IEC 27001:2005)*	Proyecto propuesto
AI1.1	A,10,5,1 Se deben hacer copias de respaldo de la información y del software, y se deben poner a prueba con regularidad de acuerdo con la política de respaldos adecuada. A,10,1.1 Los procedimientos de operación se deben documentar, mantener y estar disponibles para todos los usuarios que los necesiten.	Disponer de un equipo para contingencia en la empresa o site alterno
AI25.2	A.6.1.5. Se deben identificar y revisar con regularidad los requisitos de confidencialidad o los acuerdos de no divulgación que reflejan las necesidades de la organización para la protección de la información. A.10.1.3. Las funciones y las áreas de responsabilidad se deben distribuir para reducir las oportunidades de modificación no autorizada o no intencional, o el uso inadecuado de los activos de información A.10.7.3. Se deben establecer procedimientos para el manejo y almacenamiento de la información con el fin de proteger dicha información contra divulgación no autorizada o uso inadecuado.	Definir responsabilidades y establecer niveles de autorización para aprobaciones de créditos.

Cuadro 6-17 Controles propuestos para los activos de referencia Anexo A de la ISO/IEC 27002:2005[A]

6. **Determinar el nivel de exposición detallado por cada activo de información:** Según los criterios propuestos por la Guía de Administración de Riesgos de Microsoft[1] para determinar el nivel de exposición detallado, la empresa ha definido que el impacto a la *confidencialidad e integridad* que causaría la amenaza identificada en los activos de referencia:

   - **AI.1. Directorio Activo:** En cuanto a la *confidencialidad e integridad (cuadro 4-10),* provocaría pérdidas moderadas **(Nivel de Exposición 3)**, ocasionando costos operativos y reduciendo ingresos al impedir que los usuarios ingresen a su información de manera habitual. Por otro lado, habiendo implementado la ISO/IEC 27001:2005, el nivel de exposición detallado se mantendría en el **Nivel de exposición 3**, ya que las pérdidas y daños en cuanto a confidencialidad e integridad se mantienen moderados. Para el resto de activos el nivel de exposición puede variar, teniendo varias afectaciones por la implementación de la ISO/IEC 27001:2005.

     En cuanto a la *disponibilidad* de la información *(cuadro 4-11),* el nivel de exposición de la amenaza aumenta los costos del soporte técnico y se generan retrasos en los compromisos de negocios al imposibilitar la utilización de los accesos al dominio de la empresa y a la información contenida en cada una de sus cuentas. Esta afectación corresponde al **Nivel de Exposición 4**. Con la implementación de la ISO/IEC 27001:2005, el nivel de exposición en cuanto a disponibilidad disminuye al **Nivel de Exposición 3**.

     Siguiendo la sugerencia de la Guía de Administración de Riesgos de Microsoft[1] de seleccionar el mayor valor entre los dos criterios, **el nivel de exposición para este activo corresponde a 4 sin la ISO/IEC 27001:2005 y 3 con la ISO/IEC 27001:2005**.

   - **AI.25.2 Datos de clientes y créditos:** En cuanto a la *confidencialidad e integridad (cuadro 4-10)* provocaría daños graves **(Nivel de exposición 4)**, afectando a la rentabilidad o al éxito de la empresa, siendo visibles externamente. Implementado la ISO/IEC 27001:2005, el nivel de exposición detallado bajaría al **Nivel de Exposición 3**, ya que las pérdidas y daños en cuanto a confidencialidad e integridad se mantienen moderados.

En cuanto a la *disponibilidad* de la información *(cuadro 4-11)*, el nivel de exposición de la amenaza aumenta los costos del soporte y se generan retrasos en los compromisos del negocio al no disponer de la información de crédito adecuada. Esta afectación corresponde al **Nivel de Exposición 4**. Con la implementación de la ISO/IEC 27001:2005, el nivel de exposición en cuanto a disponibilidad disminuye al **Nivel de Exposición 3**.

Siguiendo la sugerencia de la Guía de Administración de Riesgos de Microsoft[1] de seleccionar el mayor valor entre los dos criterios, **el nivel de exposición para este activo corresponde a 4 sin la ISO/IEC 27001:2005 y 3 con la ISO/IEC 27001:2005.**

El cuadro a continuación resume el Nivel de Exposición determinado para cada uno de los activos de referencia:

Situación actual: sin ISO/IEC 27001:2005

No. Activo *(cuadros 6-01 y 6-02)*	[A] Confidencialidad o integridad *(cuadro 4-10)*	[B] Disponibilidad *(cuadro 4-11)*	Nivel de Exposición Detallado *(mayor valor entre [A] y[B])*
AI1.1	3	4	**4**
AI25.2	4	4	**4**

Cuadro 6-18 Nivel de exposición detallado sin la ISO/IEC 27001:2005[A]

Situación proyectada: con ISO/IEC 27001:2005

No. Activo *(cuadros 6-01 y 6-02)*	[A] Confidencialidad o integridad *(cuadro 4-10)*	[B] Disponibilidad *(cuadro 4-11)*	Nivel de Exposición Detallado *(mayor valor entre [A] y[B])*
AI1.1	3	3	**3**
AI25.2	3	3	**3**

Cuadro 6-19 Nivel de exposición detallado con la ISO/IEC 27001:2005[A]

La información del Nivel de Exposición Detallado de todos los activos se encuentra disponible en el Anexo F-01 del presente documento.

7. **Determinar el nivel de impacto detallado por cada activo de información:** El nivel de impacto se calcula en base al impacto identificado en la fase de recopilación de información *(punto 6.1)* y el factor de exposición del activo *(cuadro 4-12)*.

- **AI.1. Directorio Activo:** La empresa considera que una falla del servidor dañaría la mayor parte del activo, por lo que sin la implementación de la ISO/IEC 27001:2005, el Nivel de Exposición 4 *(cuadro 6-18)* equivale al 80%. Con la implementación de la ISO/IEC 27001:2005, el Nivel de Exposición 3 *(cuadro 6-19)* disminuye al 60%.

- **AI.25.2 Datos de clientes y créditos:** La empresa considera que la falta de confiabilidad en la información de clientes y crédito dañaría la mayor parte del activo, por lo que sin la implementación de la ISO/IEC 27001:2005, el nivel de exposición 4 *(cuadro 6-18)* equivale al 80%. Con la implementación de la ISO/IEC 27001:2005, el nivel de exposición 3 *(cuadro 6-19)* disminuye al 60%.

El producto del Factor de Exposición con el Impacto al negocio determinado en la fase anteriormente nombrada, es el nivel de Impacto Detallado.

Situación actual: sin ISO/IEC 27001:2005

No. Activo *(cuadro 6-01 y 6-02)*	Impacto al Negocio *(cuadro 6-03)*	Nivel de exposición *(cuadro 6-18)*	Factor de Exposición *(cuadro 4-12)*	Nivel de Impacto Detallado *(cuadro 4-13)*
AI1.1	**10**	4	**0,8**	**8**
AI25.2	**10**	4	**0.8**	**8**

Cuadro 6-20 Nivel de impacto detallado sin la ISO/IEC 27001:2005[A]

Situación proyectada: con ISO/IEC 27001:2005

No. Activo *(6-01 y 6-02)*	Impacto al Negocio *(cuadro 6-03)*	Nivel de exposición *(cuadro 6-19)*	Factor de Exposición *(cuadro 4-12)*	Nivel de Impacto Detallado *(cuadro 4-13)*
AI1.1	**10**	3	**0,6**	**6**
AI25.2	**10**	3	**0,6**	**6**

Cuadro 6-21 Nivel de impacto detallado con la ISO/IEC 27001:2005[A]

La información del Impacto Detallado de todos los activos sin la ISO/IEC 27001:2005 y con la ISO/IEC 27001:2005 se encuentra disponible en los Anexos F-01 y F-02 respectivamente del presente documento.

8. **Determinar la probabilidad del impacto detallado por cada activo de información:** Se utiliza la plantilla propuesta por la Guía de Administración de Riesgos Microsoft[1] para facilitar el cálculo de la probabilidad del impacto para el activo AI1.1, servicio de Active Directory, en la que se ha incluido la probabilidad de vulnerabilidad tanto en el entorno del activo como en función de la efectividad de los controles actuales.

Atributos de Probabilidad de ocurrencia de las vulnerabilidades en su entorno *(seleccionar una)*	Situación Actual: sin ISO/IEC 27001:2005		Situación Proyectada: con ISO/IEC 27001:2005	
	AI1.1	**AI25.2**	**AI1.1**	**AI25.2**
Alta (Calificar con "5" si cualquiera aplica) • Existe una población grande de atacantes (aficionados) • Se puede ejecutar de forma remota • Se necesitan privilegios anónimos • Método de aprovechamiento publicado externamente • Automatizado				
Media (Calificar con "3" si cualquiera aplica) • Existe una población mediana de atacantes (expertos especialistas) • No se puede ejecutar remotamente • Se necesitan privilegios de nivel de usuario • Método de aprovechamiento no público • No automatizado	✓	✓		
Baja (Calificar con "1" si cualquiera aplica) • Existe una población pequeña de atacantes (conocimiento interno) • No se puede ejecutar remotamente • Se necesitan privilegios de nivel de administrador • Método de aprovechamiento no público • No automatizado			✓	✓
[A] = Probabilidad de vulnerabilidad ***(según su entorno)***	**3**	**3**	**1**	**1**

Atributos de Probabilidad para las Vulnerabilidades según la efectividad de sus controles **Calificación:** ***(SI = 1; NO = 0)***	**Situación actual: sin ISO/IEC 27001:2005**		**Situación proyectada: Con ISO/IEC 27001:2005**	
	AI1.1	**AI25.2**	**AI1.1**	**AI25.2**
¿El control se ha definido y cumplido de forma eficaz?	**1**	**1**	**0**	**1**
¿La toma de conciencia se comunica y sigue de forma eficaz?	**0**	**1**	**0**	**1**
¿Los procesos se han definido y puesto en práctica de forma eficaz?	**1**	**1**	**0**	**0**
¿La tecnología o los controles existentes reducen la amenaza de forma eficaz?	**1**	**1**	**0**	**0**
¿Son suficientes las prácticas de auditoría actuales para detectar abusos o deficiencias de control?	**1**	**1**	**1**	**0**
[B] = Probabilidad de ocurrencia de la vulnerabilidad ***(según la efectividad de sus controles)***	**4**	**5**	**1**	**2**
Probabilidad de ocurrencia del Impacto	**7**	**8**	**2**	**3**

Cuadro 6-22 Probabilidad de impacto detallado[A]

La información de la Probabilidad de Ocurrencia del Impacto Detallado de todos los activos sin la ISO/IEC 27001:2005 y con la ISO/IEC 27001:2005 se encuentra disponible en los Anexos F-01 y F-02 respectivamente del presente documento.

9. **Determinar el nivel de riesgo detallado.** El nivel de riesgo detallado es el resultado del cruce entre el nivel de impacto y la probabilidad de ocurrencia previamente determinados por la empresa.

- **AI.1. Directorio Activo:** El nivel de riesgo del activo de información sin la ISO/IEC 27001:2005 es ALTO, lo cual implica que el activo de información requiere de un nivel prioritario de urgencia para la implementación de controles de mitigación de la amenaza identificada. Con la implementación de la ISO/IEC 27001:2005 el nivel de riesgo disminuye claramente a nivel BAJO.

- **AI.25.2 Datos de clientes y créditos:** El nivel de riesgo del activo de información sin la ISO/IEC 27001:2005 es ALTO, lo cual implica que el activo de información requiere de un nivel prioritario de urgencia para la implementación de controles de mitigación de la amenaza identificada. Con la implementación de la ISO/IEC 27001:2005 el nivel de riesgo disminuye a nivel BAJO.

El siguiente cuadro resume el Nivel de Riesgo Detallado para los dos activos de referencia:

Situación actual: sin ISO/IEC 27001:2005

AI1.1

AI25.21

Nivel de Impacto *(cuadro 6-20)*		Nivel de Riesgo De ado										
	10	0	10	20	30	40	50	60		80	90	100
	9	0	9	18	27	36	45	54		72	8	90
	8	0	8	16	24	32	40	48	**56**	**64**		
	7	0	7	14	21	28	35	42	49	56	63	70
	6	0	6	12	18	24	30	36	42	48	54	60
	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
	1	0	1	2	3	4	5	6	7	8	9	10
		0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
		Probabilidad de ocurrencia del impacto *(cuadro 6-22)*										

Cuadro 6-23 Nivel de riesgo detallado sin ISO/IEC 27001:2005[1]

Situación proyectada: con ISO/IEC 27001:2005

		Nivel de Riesgo Detallado										
Nivel de impacto *(6-21)*	**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		14	21	28	35	42	49	56	63	70
	6			**12**	**18**							
	5	0		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
	1	0	1	2	3	4	5	6	7	8	9	10
		0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
		Probabilidad de ocurrencia del impacto *(cuadro 6-22)*										

AI1.1 → AI25.2

Cuadro 6-24 Nivel de riesgo detallado con ISO/IEC 27001:2005[1]

En los Anexos F-01 y F-02 se encontrará una la lista de prioridades de riesgo sin la ISO/IEC 27001:2005 y con la ISO/IEC 2001:2005 respectivamente.

Como se observa en los Anexos, los activos con nivel de riesgo detallado ALTO sin la implementación de la ISO/IEC 27001:2005 disminuyeron a niveles de riesgo detallado MODERADO y en la mayoría a niveles BAJO con la implementación de la ISO/IEC 27001:2005.

En la evaluación de riesgos Cuantitativo se cuantificarán aquellos activos que tengan un nivel de riesgo ALTO y MODERADO antes de la implementación de la ISO/IEC 27001:2005. Aquellos activos que muestren un nivel de riesgo bajo, deberán ser tomados en cuenta en una etapa posterior.

6.3. Evaluación de Riesgos Cuantitativa

Una vez realizada la evaluación del riesgo cualitativo, se asignará un valor monetario a cada uno de los activos con nivel de riesgo ALTO y MODERADO. A continuación, se seguirán los pasos descritos en el punto 4.4.2 del capítulo IV para llegar a este fin.

1. **Asignar un valor monetario a cada clase de activos de la organización:** Para determinar los valores directos e indirectos de la pérdida de un activo, se ha realizado una distribución en función de las ventas del año 2011, que tienen un valor de 275 millones de dólares:

Categorización de Activos	Distribución ventas %	Ventas 2011 $
ACTIVOS CON RIESGO ALTO	60%	165.000.000
VALORES DIRECTOS	70%	115.500.000
VALORES INDIRECTOS	30%	49.500.000
ACTIVOS CON RIESGO MEDIO Y BAJO	40%	110.000.000
TOTAL VENTAS ANUALES 2011		275.000.000

Cuadro 6-25 Categorización de activos para determinar los valores directos e indirectos[A]

1.1. A continuación calculará el valor de los activos con nivel de riesgo ALTO y moderado, resultado de la Evaluación Cualitativa *(punto 6.2).*

a) Valores Directos: Para los dos activos de referencia se han asignado Valores Directos de la siguiente manera:

- **AI.1. Directorio Activo:** Se le ha asignado un valor en base a la subcategoría "valor físico", donde el activo tiene un peso del 5%. Además, la categoría "valor físico" tiene un peso de 10%, siendo:

  115.500.000 x 5% x 10% = 577.500 dólares.

- **AI.25.2 Datos de clientes y créditos:** Se le ha asignado un valor en base a las subcategorías "valor empresa", donde el activo tiene un peso del 10%, "valor usuarios", donde el activo tiene un valor del 10%, "propiedad intelectual" con un valor del 10%. Además, las dos categorías tienen de por sí un peso del 40%, 30% y 15% respectivamente, siendo:

  115.500.000 x 10% x 40% +
  115.500.000 x 10% x 30% +
  115.500.000 x 10% x 15% =
  9.817.500 dólares

A continuación se presenta un resumen de la asignación de Valores Directos para los activos de referencia:

Activo	Valores Directos					Total Valor Directo
	Valor físico	Valor empresa	Valor usuarios	Propiedad intelectual	Otros valores	
	10%	40%	30%	15%	5%	
AI1.1	577.500	-	-	-	-	577.500
A25.1.2		4620.000	3465000	1732500		9.817.500

Cuadro 6-26 Asignación de Valor Directo a activos utilizados como referencia[A]

b) Valores Indirectos: Para los dos activos de referencia se han asignado Valores Directos de la siguiente manera:

- **AI.1. Directorio Activo:** Se ha asignado al activo un Valor Indirecto en base a la subcategoría "otros valores", donde el activo tiene un peso del 5%. Además, la categoría "otros valores" tiene un peso de 5%, siendo:

  49.500.000 x 5% x 5% = 123.750 dólares.

- **AI.25.2 Datos de clientes y créditos:** Se ha asignado al activo un Valor Indirecto en base a las subcategorías "valor para la competencia", donde el activo tiene un peso del 15% y "valoración de mercado", con un peso de 15%. Además, las dos categorías tienen un peso de 15% y 40% respectivamente, siendo:

  49.500.000 x 15% x 15% +
  49.500.000 x 15% x 40% =
  4.083.750 dólares

A continuación se presenta un resumen de la asignación de Valores Indirectos para los activos de referencia:

No. Activo	Valores Indirectos					Total Valor Directo
	Mejora de productividad	Valor para la competencia	Valoración de Mercado	Marca	Otros valores	
	20%	15%	40%	20%	5%	
AI1.1	-	-	-	-	123.750	123.750
AI25.2		1.113.750	2.970.000			4.083.750

Cuadro 6-27 Asignación de Valor Indirecto al activo utilizado como referencia[A]

c) Inversión en la compra, implementación e instalación: La empresa estima que ha invertido tanto en la compra, como en la implementación y estabilización del servicio de Directorio Activo un valor de 9.878,48 dólares. En el caso de Datos de clientes y crédito la empresa ha tenido pérdidas por un valor de 1.166.000 dólares

Por tanto el valor de los activos se presenta en:

AI1.1: 701.250 dólares – 9.880 dólares = 691.372 dólares

AI25.2: 13.901.250 dólares – 1.166.000 dólares = 12.735.250 dólares

1.2. El resultado final es un listado de activos con el desglose de costos y valores para determinar su costo global. A continuación se presenta un extracto del listado con los datos de los activos AI1.1 y AI25.2, que se están tomando como referencia.

No. Activo *(cuadro (6-01 y 6-02)*	Impacto al negocio	Compra	Instalación	Implementación	Customización	Otros Costos	Valor Físico	Valor para la Empresa	Valor para los Usuarios	Propiedad Intelectual	Otros Valores	Mejora de la Productividad	Valor para la Competencia	Valoración del Mercado	Marca	Otros Valores	Otros Valores	Valor Total del Activo
		Costos (Valores Negativos)					**Valores Directos**					**Valores Indirectos**					**Otros**	**Total**
AI1.1	ALTO	3,80	0,00	2,83	0,00	3,25	577,50	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	123,75	0,00	**691.372**
AI25.2	ALTO	0,00	0,00	0,00	0,00	1166	0,00	4620	3465	1732,5	0,00	0,00	1113,75	2970	0,00	0,00	0,00	**1.2735.250**

Cuadro 6-28 Cuantificación del activo utilizado como referencia[A]

En el Anexo G se encuentra el resto de activos con sus respectivos valores monetarios.

1.3. Luego de haber cuantificado cada uno de los activos, se asigna un solo valor monetario por clase de activo en cuanto a su Impacto para el negocio (10- Alto, 5 - Medio). El resultado global es el siguiente:

	Impacto al negocio	Valor Monetario
10	**HBI - Impacto al Negocio Alto**	**247.500**
5	**MBI - Impacto al Negocio Medio**	**685.110**

Cuadro 6-29 Valoración por clase de activo de Impacto al Negocio[A]

Para el caso de los activos en análisis, los cuales tienen un Impacto al Negocio ALTO (10), se tomaría como valor de referencia asignado, 247.500 dólares.

El valor total de los activos es de **160.782.825** dólares.

En el Anexo G se encuentra la valoración total de los activos de la empresa.

2. Determinar el impacto financiero inmediato de la pérdida del activo: Para calcular la fórmula planteada en el capítulo IV para determinar el impacto financiero de la pérdida del activo, se tiene siguen los siguiente pasos:

2.1. Determinar el valor de expectativa de pérdida simple - SLE:

Al multiplicar el factor de exposición obtenido en la evaluación cualitativa antes de la implementación de la ISO/IEC 27001:2005 *(cuadro 6-20)* y con la implementación de la misma *(cuadro 6-21)* por el valor de la clase del activo según su Impacto al Negocio *(cuadro 6-29)*, se podrá predecir que las pérdidas directamente atribuibles en este caso serían:

Situación actual: sin ISO/IEC 27001:2005

AI1.1 247.500 dólares * 80% = **198.000** dólares.

AI25.2 247.500 dólares * 80% = **198.000** dólares.

Situación proyectada: con ISO/IEC 27001:2005

AI1.1 247.500 dólares * 60% = **148.500** dólares.
AI25.2 247.500 dólares * 60% = **148.500** dólares

2.2. Valor de probabilidad de ocurrencia anual - ARO:

La probabilidad de ocurrencia de la amenaza - ARO es calculada en función del número de veces que la amenaza puede ocurrir en un año *(cuadro 4-17)*.

Para los dos activos de referencia se tiene:

Situación actual: sin ISO/IEC 27001:2005

AI1.1 Probabilidad de Ocurrencia= 1 vez / 3 años= **0,33** veces/año
AI25.2 Probabilidad de Ocurrencia= 3 veces / 3 años= **1** veces/año

Situación proyectada: con ISO/IEC 27001:2005

AI1.1 Probabilidad de Ocurrencia= 0.5 veces / 3 años= **0,17** veces/año
AI25.2 Probabilidad de Ocurrencia= 1 vez / 3 años= **0,33** veces/año

2.3. Valor de expectativa de pérdida anual - ALE:

Aplicando la fórmula propuesta en el capítulo IV *(4.4.2 punto 2)*, la Expectativa de Pérdida Anual – ALE que pueden sufrir los activos se estima así:

- **AI.1. Directorio Activo:** La expectativa de pérdida anual de la amenaza de que una falla en el servidor inutilice el Directorio Activo de la empresa es de 66.000 dólares y después de implementar la ISO/IEC 27001:2005, se disminuye a 24.750 dólares.

- **AI.25.2 Datos de clientes y créditos:** La expectativa de pérdida anual de la amenaza de fallas por alteración de datos y fraudes afecten la disponibilidad e integridad de la información de crédito de la empresa es de 198.000 dólares y después de implementar la ISO/IEC 27001:2005, se disminuye a 49.500 dólares.

Situación actual: sin ISO/IEC 27001:2005

AI1.1 Daño o pérdida= 247.500 USD * 80% * 0,33 veces/año= 66.000 USD

AI25.2 Daño o pérdida= 247.500 USD * 80% * 1 veces/año= 198.000 USD

No. Activo *(cuadros 6-01 y 6-02)*	**Impacto al Negocio** *(cuadro 6-03)*	**Factor de Exposición: [FE]** *(cuadro 6-20)*	**Valor de la Clase de Activo de Impacto al Negocio: [VA]** *(cuadro 6-29)*	**Expectativa de Pérdida Simple: [SLE]** *(FE * VA)* *(2.2. de la presente sección)*	**Tasa Anual de Ocurrencia: [ARO]** *(2.2. de la presente sección)*	**Valor de Expectativa de Pérdida Anual: [ALE]** *(SLE * ARO)*
AI1.1	10	0,8	247.500	198.000	0,33	**66.000**
AI25.2	10	0,8	247.500	198.000	1,00	**198.000**

Cuadro 6-30 Valoración por clase de activo de Impacto al Negocio sin ISO/IEC 27001:2005[A]

Situación proyectada: con ISO/IEC 27001:2005

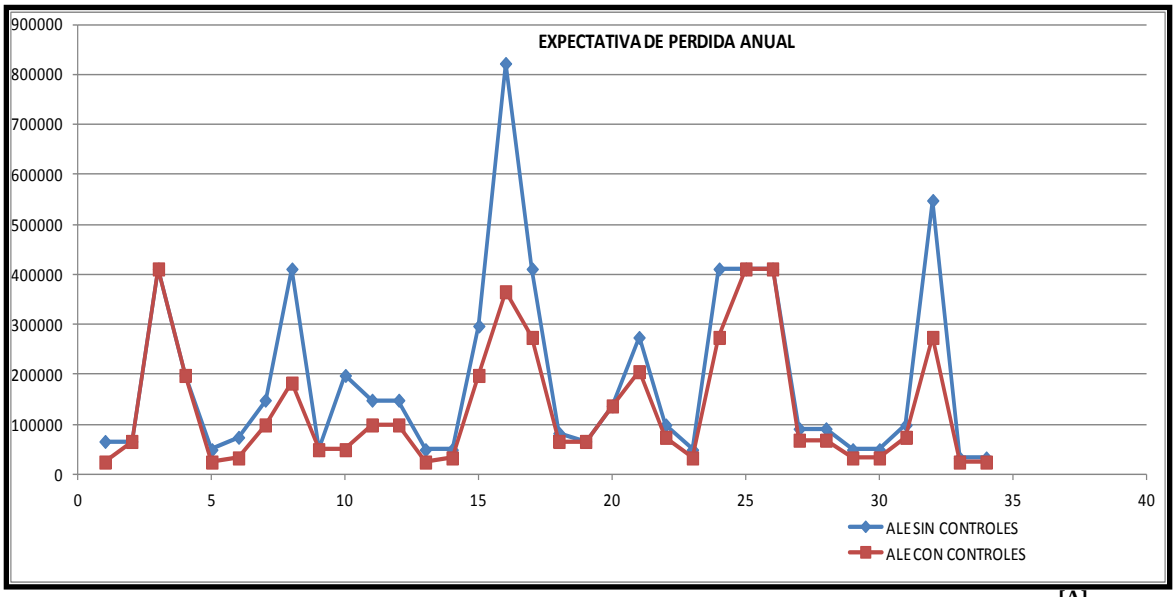
AI1.1 Daño o pérdida= 247.500 USD * 60% * 0,17 veces/año= 24.750 USD

AI25.2 Daño o pérdida= 247.500 USD * 60% * 0,33 veces/año= 49.500 USD

No. Activo *(cuadros 6-01 y 6-02)*	**Impacto al Negocio** *(cuadro 6-02)*	**Factor de Exposición: FE** *(cuadro 6-09)*	**Valor de la Clase de Activo de Impacto al Negocio: VA** *(cuadro 6-16)*	**Expectativa de Pérdida Simple: SLE** *(FE * VA)* *(2.2. de la presente sección)*	**Tasa Anual de Ocurrencia: ARO** *(2.2. de la presente sección)*	**Valor de Expectativa de Pérdida Anual: ALE** **(SLE * ARO)**
AI1.1	10	0,6	247.500	198.500	0,17	**24.750**
AI25.2	10	0,6	247.500	198.500	0,33	**49.500**

Cuadro 6-31 Valoración por clase de activo de Impacto al Negocio con ISO/IEC 27001:2005[A]

De manera gráfica (en base a los datos del Anexo H) podemos revisar como la aplicación de controles genera beneficio al disminuir el valor del riesgo en la mayoría de los 34 activos críticos evaluados de manera cuantitativa:



Cuadro 6-32 Comparativo del riesgo sin control y con control por activo[A]

A nivel de totales, tenemos los siguientes resultados:

Situación actual: sin ISO/IEC 27001:2005

Expectativa de Pérdida Simple (SLE) *(2.2. de la presente sección)*	**Valor de Expectativa de Pérdida Anual (ALE)** *(cuadro 6-17)*
9.056.280	**6.534.063**

Cuadro 6-33 Expectativa de pérdida simple y anual sin ISO/IEC 27001:2005[A]

Situación proyectada: con ISO/IEC 27001:2005

Expectativa de Pérdida Simple : SLE *(2.2. de la presente sección)*	**Valor de Expectativa de Pérdida Anual : ALE** *(6-18)*
7.826.748	**4.510.245**

Cuadro 6-34 Expectativa de pérdida simple y anual con ISO/IEC 27001:2005[A]

En los Anexos H-01 y H-02 se encontrarán los listados de todos los activos con la Expectativa de Pérdida Anual.

3. Determinación del costo de los controles:

Según la oferta de Bureau Veritas, el costo del proyecto de implementación de la ISO/IEC 27001:2005 es de 24.000 dólares, con los costos adicionales el proyecto se estima costará: 45.650 dólares. A continuación un desglose:

Costo estimado del Soporte Técnico			
Personal	**Costo estimado mensual**	**Horas**	**Costo estimado por hora**
Soporte de Sistemas	2.000	240	8,33
Gerencia	4.000	240	16,67
Dirección	10.000	240	41,67

Cuadro 6-35 Resumen costos de implementación ISO/IEC 27001[A]

PROYECTO ISO 27001:2005			
Rubros	**Cantidad**	**Valor unitario**	**Total**
Proyecto ISO	1	24.000,00	24.000
Transporte-alimentación	1	24.00,00	2.400
Soporte de Sistemas	1.440	8,33	12.000
Gerencia	60	16,67	1.000
Dirección	30	41,67	1.250
Otros costos	1	5.000,00	5.000
Total			**45.650**

Cuadro 6-35 Resumen costos de implementación ISO/IEC 27001[A]

El costo total de la ISO/IEC 27001:2005 y los controles a implementar es de: **747.076 dólares.**

En el Anexo I se podrá observar el desglose y obtención de esta cifra.

6.4. Evaluación Costo Beneficio

Aplicando la fórmula para el cálculo de ROSI propuesta por la Guía de Administración de Riesgos de Seguridad de Microsoft[1] el Retorno de la Inversión de Seguridad es de **189 %**, tal como se expresa en el siguiente adjunto:

SUMARIO DE VALORES PARA ANALISIS ROSI	
ALE sin controles	6.534.063
ALE con controles	4.510.245
Riesgo disminuido	2.023.818
Costo de aplicación de controles	701.426
Riesgo disminuido = Beneficio	1.322.392
ROSI = [(ALE antes de controles - ALE después de controles) – Costo anual de los controles/Costo anual de los controles	**1,89**

Cuadro 6-36 Cálculo de ROSI[A]

De la información cuantificada y del cálculo del ROSI, se obtienen algunas relaciones importantes:

1. **Relación de Inversión**

Costo de aplicación de controles	701.426
ROSI (Valor) = Beneficio – costo	1.322.392
Relación	**1,89**

Cuadro 6-37 Relación de Inversión[A]

De la información presentada se establece que al invertir 701.426 dólares se logra una disminución del nivel de riesgo de 1.322.392 dólares lo cual significa un retorno de la inversión en seguridad de la información (ROSI) del 189 %. En otras palabras por cada dólar que se invierta en seguridad se logra disminuir en 1,89 dólares el nivel de riesgo en la empresa.

2. **Relación de riesgo disminuido sobre riesgo inicial**

Cuantificación del riesgo sin controles	6,534,063
Cuantificación del riesgo con controles	4,510.245
Relación	**30,97%**

Cuadro 6-38 Relación de riesgo disminuido sobre riesgo inicial[A]

Invirtiendo 701.426 dólares se logra una disminución del riesgo de un 30,97%

3. **Relación Beneficio sobre el riesgo**

ROSI (Valor) = Beneficio – costo	1.322.392
Cuantificación del riesgo sin controles	6.534.063
Relación	**20,24%**

Cuadro 6-39 Relación Beneficio sobre el riesgo[A]

El beneficio obtenido al invertir en un proyecto de Seguridad de la Información es de un 20.24 % respecto al riesgo total sin controles.

4. **Relación de inversión respecto al riesgo**

Costo de aplicación de controles	701.426
Cuantificación del riesgo sin controles	6.534.063
Relación	**10,73%**

Cuadro 6-40 Relación de Inversión respecto al riesgo[A]

Con una inversión del 10,73% respecto al total del riesgo sin controles, se logra una reducción del nivel de riesgo de 1.322.392 dólares.

En resumen mientras el ROI financiero evalúa cuánto dinero se ganará por realizar una inversión, el ROSI nos indica cuánto dinero se dejará de perder, el resultado obtenido es positiva por cuanto al invertir en controles, el nivel de riesgo tiende a disminuir.

CAPÍTULO VII: CONCLUSIONES Y RECOMENDACIONES

Como cierre del presente estudio, se entregan las respectivas conclusiones y recomendaciones:

7.1. Conclusiones

En relación al primer objetivo específico planteado en la presente Tesis para evidenciar la importancia de la seguridad de la información en las empresas, se presentan las siguientes conclusiones:

- La información considerada como un factor productivo es un recurso clave al nivel de la producción de bienes y servicios, es un recurso indispensable para las organizaciones, que necesita ser gestionado. (1.2)
- La utilidad de la información y su valor en las organizaciones la convierten en un elemento que requiere ser asegurado y protegido de ataques, modificaciones indebidas, minimizando la afectación a su disponibilidad, integridad y confiabilidad.(2.1)
- Las empresas, independiente de su tamaño, que no disponen de procesos, de mecanismos y técnicas que mitiguen sus riesgos y garanticen una alta disponibilidad de las operaciones de su negocio, entre ellas la gestión, protección y aseguramiento de su información, tienden a caminar hacia el fracaso.(2.2)
- La seguridad de la información se vuelve fundamental y se corrobora con cifras estadísticas donde entre otros valores importantes nos dicen: el 94% de empresas cerrarán a los 2 años de una pérdida severa de la información en sus sistemas, el 70% no sobreviviría a más de 4 días sin sus datos, el 55% de los problemas son por error humano. (2.2)
- Una iniciativa colombiana ha empezado a medir cómo las empresas se encuentran respecto a la seguridad de la información en Latinoamérica, observando que cada vez se destinan mayores presupuestos, que aún existe desconocimiento, que los incidentes tienden a disminuir, que se están utilizando algunas alternativas de estándares. Es lamentable observar como dentro de esas cifras el Ecuador no aparece.(2.3)

El segundo objetivo específico planteado de investigar y conocer sobre las técnicas de seguridad y requerimientos que exige la norma ISO/IEC 27001:2005, genera las siguientes conclusiones:

- El objetivo principal de la ISO/IEC 27001:2005 es garantizar la confidencialidad, disponibilidad, e integridad de la información de la empresa para que ésta cumpla con los objetivos del negocio principalmente.
- La ISO/IEC 27001:2005[J] se enfoca en temas estrictamente estratégicos, debiendo ser de especial interés para los Altos Mandos de todo tipo de empresa.
- La ISO/IEC 27001:2005[J] adopta un proceso para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el SGSI en una organización. Adopta también el modelo de Ciclo de Mejora Continua "Plan-Do-Check-Act" (PDCA), el cual es aplicado a toda la estructura de procesos de SGSI , y significa lo siguiente:
    - Plan (Establecer el SGSI): Implica establecer la política del SGSI, sus objetivos, procesos, procedimientos relevantes para la administración de riesgos y mejoras para la seguridad de la información, entregando resultados acordes a las políticas y objetivos de toda la organización.
    - Do (Implementar y operar el SGSI): Representa la forma en que se debe operar e implementar la política, controles, procesos y procedimientos.
    - Check (Monitorear y revisar el SGSI): Implica analizar y medir donde sea aplicable, los procesos ejecutados con relación a la política del SGSI, evaluar objetivos, experiencias e informar los resultados a la administración para su revisión.
    - Act (Mantener y mejorar el SGSI): Realizar las acciones preventivas y correctivas, basados en las auditorías internas y revisiones del SGSI o cualquier otra información relevante para permitir la continua mejora del SGSI.
- La norma exige entre los aspectos más importantes:
    - Compromiso y apoyo de los Altos Mandos de la empresa a través de la conformación de comités de Dirección para la propuesta de acciones de mejora e identificación continua de no conformidades.
    - Definición clara de un alcance apropiado con el negocio.
    - Concienciación y formación de todo el personal de la empresa orientado hacia la seguridad.

- Evaluación exhaustiva y adecuada de riesgos para la empresa. Creación de un sistema de gestión de incidentes que recopile notificaciones por parte de usuarios.
- Compromiso de mejora continua por parte de todo el personal de la empresa.
- Establecimiento de políticas y normas que regulen la seguridad de la información en la empresa.
- Organización y comunicación entre todas las áreas de la empresa.
- Integración del SGSI en la empresa mediante la participación de todo el personal.

Como conclusión de la segunda hipótesis planteada, la aplicación de controles formales basados en estándares fundamentados en las mejores prácticas como la ISO/IEC 27001:2005 facilitan la generación de proyectos de mejoramiento, que permiten la consecución de beneficios cualitativos y cuantitativos muy importantes para la empresa. De esta forma el estándar ISO/IEC 27001:2005 se orienta en garantizar la disponibilidad, confidencialidad e integridad de la información, mediante normativas que aportan mejores prácticas contra el aprovechamiento inadecuado de amenazas y vulnerabilidades, sin presentar una metodología orientada a garantizar la continuidad del negocio.

El tercer objetivo específico de analizar la situación actual de la empresa, sus principales necesidades de seguridad y costos incurridos por brechas de seguridad, se presentan las siguientes conclusiones:

- La empresa analizada es líder en su industria, ha experimentado en los últimos diez años un crecimiento muy importante en muchos aspectos de su negocio: líder en el mercado nacional en negocio, volúmenes de ventas con records en la historia del negocio entre los años 2008 al 2011, número de empleados, número de sucursales de 1 a 9. (5.3)
- Su estrategia de negocio cambia desde el año 2008, de ser un importador de materia prima hacia el principal reciclador de material ferroso en el país, invirtiendo en una planta de fundición de acero e ingresando al mercado nacional e internacional con la compra de chatarra ferrosa.(5.3)
- En cuanto a tecnología de información, la empresa ha experimentado cambios y crecimientos muy importantes: de sistemas de desarrollo interno al software empresarial BaaN-ERP, de la empresa americana INFOR, actualmente da un nuevo avance en esta tecnología al firmar con la empresa SAP. En cuanto al correo electrónico se cambió de

Lotus Notes de IBM hacia Microsoft Exchange. Como solución de Inteligencia de Negocios, se utiliza QlikView. El número de usuarios en los últimos diez años ha tenido un crecimiento del 233.33%. Esto fundamenta cómo la organización ha ido requiriendo del apoyo tecnológico para su gestión.(5.3)

- La empresa ha realizado inversiones importantes para la obtención de las siguientes certificaciones: ISO 9001, ISO14001 y OHSAS 18001.(5.3)
- En comparación con los resultados de la III Encuesta Latinoamericana de Seguridad de la Información, la empresa muestra un patrón de comportamiento muy similar al promedio y en algunos casos resultados menores a los promedios de la encuesta. Dentro de esto se puede mencionar: no se dispone de un presupuesto para seguridad de información, un sistema de Gestión de la Seguridad de la Información, una política de seguridad, planes de capacitación en seguridad, una metodología formal para la identificación de riesgos. Sus mayores incidentes se han presentado por fraudes, software no autorizado, virus. Los principales obstáculos están en el poco entendimiento en su interior de los beneficios de la seguridad de la información.(5.4)
- La función de seguridad de la información no está considerada como una tarea principal. Las funciones de administración de seguridad son algunas de las responsabilidades a cargo del Administrador de Redes y Comunicaciones.(5-4)
- La estabilidad de la empresa se ha puesto en riesgo por alteraciones de datos y fraudes, en especial en el área de crédito y cobranzas donde su nivel de riesgo supera el millón de dólares. En general, los incidentes a lo largo de la historia reciente de esta empresa representan alrededor de 2 millones de dólares en pérdidas, pudiendo evitarse esta alta cantidad de pérdidas monetarias con la implementación de controles de seguridad más rígidos y ajustado a las necesidades de la empresa.

Además, como conclusión de la primera hipótesis planteada, el estándar ISO/IEC 27001:2005, más difundido en otros países, en Ecuador y otros países latinoamericanos, con excepción de Colombia que dispone de 11 certificaciones, constituye una práctica de seguridad poco utilizada. En el país al momento solo existen 2 empresas del sector de las Telecomunicaciones certificadas en el estándar ISO/IEC 27001:2005 (SGSI). (5.4). Esto demuestra que en las empresas del sector industrial, como en otros, independiente de su tamaño continúan adoleciendo de un manejo formal de la seguridad de la información.

El último objetivo específico sobre alinear los requerimientos de seguridad de información de la empresa seleccionada, con la solución proporcionada en el estándar ISO/IEC 27001:2005, para definir sus costos y beneficios, presenta las siguientes conclusiones:

- El alineamiento entre el estándar ISO/IEC 27001:2005 y el costo beneficio para una empresa industrial, se fundamenta en cuatro fases integradas con la Evaluación de Riesgos que propone la Guía de Administración de Riesgos de Seguridad de Microsoft[1]:
    - Visión general de la seguridad de la información en la empresa
    - Recopilación de información sobre activos de información
    - Evaluación de riesgos cualitativa y cuantitativa
    - Análisis costo beneficio
- En la empresa se identificaron 78 activos de información a través del levantamiento de información con usuarios claves. Luego del proceso de valoración cualitativa, se tomaron aquellos que en su análisis resumido presentaron un valor de riesgo Alto. Treinta y cuatro (34) activos pasaron a la etapa de evaluación detallada y cuantitativa de riesgos con la valoración económica de cada uno para obtener los datos necesarios para el análisis costo beneficio.(6.2)
- De los 133 controles sugeridos por la norma para mitigar los riesgos, en la evaluación de los 34 activos críticos identificados se han referenciado a 69 (Anexo F-02).
- A pesar de trabajar en la disminución del riesgo (ALE) en los activos cuantificados podemos ver que en algunos su valor no ha disminuido. Esto se debe a que la medida de control aplicada no altera la tasa de ocurrencia (ARO), y al calcular el factor de exposición donde se mide el impacto en la confidencialidad, integridad y disponibilidad, su valor más alto que es el que recomienda la metodología se mantiene similar al del factor de exposición del activo sin la aplicación del control.
- El nivel de riesgo para los activos cuantificados sin la aplicación de controles llega a un valor de 6.534.063 dólares, al realizar una inversión de 701.426 dólares en controles fundamentados en la ISO/IEC 27001:2005, esta cifra baja a 4.510.245 dólares, generando una disminución del valor del riesgo en 1.322.392 dólares. Estas cifras muestran un retorno de la inversión en seguridad del 189%. Es decir que por cada dólar que se invierta en seguridad se logrará una disminución del riesgo de 1,89 dólares. Llegándose a obtener una disminución del riesgo cuantificado del 30,97%.(6.4)

Se puede concluir y reforzar el objetivo principal de este trabajo de Tesis y por lo tanto sustentar la tercera hipótesis planteada, que la aplicación de la ISO/IEC 27001:2005, sí representa un beneficio importante para la empresa, con una inversión razonable se puede obtener una disminución importante del nivel de riesgos (30,97%), además de la incorporación dentro de la organización de un estándar formal, garantizado y certificable.

7.2. Recomendaciones

- Un esfuerzo para mitigar el riesgo puede ser realizado en función de cada incidente presentado, pero el valor será mayor, si ese esfuerzo es canalizado mediante una metodología con estándares certificables, apoyados en mejores prácticas, aportando a la información de la empresa un mayor nivel de protección y un más amplio rango para mitigar el riesgo.
- Se recomienda que para este tipo de estudios se busque el apoyo de usuarios expertos que conozcan de forma exhaustiva las amenazas e historial de incidentes que afectan a la empresa en cuestión ya que caso contrario sería imposible culminarlo.
- Aunque el objetivo de esta Tesis se enfoca en la ISO/IEC 27001:2005, se recomienda obtener información relativa a la gestión de la seguridad de la información de otros métodos y marcos reconocidos.
- Luego de la revisión del Análisis Costo Beneficio de la aplicación del estándar ISO/IEC 27001:2005 a la empresa seleccionada, se debe iniciar un proceso de toma de decisiones por parte de los Altos Mandos de la empresa con el fin de implementar las medidas de mitigación de riesgos recomendadas.
- Para la implementación de la ISO/IEC 27001:2005, la empresa debe mantener la sencillez y restringirse a un alcance manejable y reducido, como por ejemplo enfocarse en un centro de procesamiento de datos, un proceso de negocio clave, o un área sensible concreta. Una vez conseguido el éxito en uno de los ítems mencionados y observados los beneficios, ampliar gradualmente el alcance en varias fases.
- Aunque la empresa no se certifique en el estándar ISO/IEC 27001:2005, se recomienda el cumplimiento de sus principios para lograr formalidad y beneficios en cuanto al manejo de la seguridad de la información dentro de la organización, aprovechando los aportes que la familia ISO/IEC 27000 presentan para las empresas.

- Es vista del beneficio establecido en el presente estudio, es importante que la empresa invierta en seguridad de la información, creando un área formal dentro de la empresa, estableciendo un presupuesto para seguridad, incentivando la definición de una política de seguridad, fomentando el camino hacia la implementación de su SGCI y por tanto planteándose la certificación en el estándar ISO/IEC 27001:2005 a mediano plazo.
- El manejo de un estándar o buenas prácticas para garantizar la disponibilidad, integridad y confiabilidad de la información dentro de una empresa, debe convertirse en una práctica de seguridad continua y formal a lo largo del tiempo. Su revisión debería ser cada uno o dos años estableciendo planes de mitigación a cumplirse para disminuir el riesgo.
- Este estudio además de mostrar el costo beneficio de un estándar para la seguridad de la información en una empresa abre una oportunidad para recomendar a que las empresas ecuatorianas a través de sus agrupaciones gremiales empiecen a concientizarse de la importancia de utilizar este tipo de estándares, como práctica formal dentro de sus empresas.
- Se recomienda que en nuestro país, el Gobierno Nacional a través de sus organismos de normalización fortalezcan e incentiven a que las empresas accedan a la utilización de estándares de seguridad de la información como parte de la aplicación de mejores prácticas dentro de las empresas.
- Recomendamos al personal docente de la Facultad de Ingeniería, Escuela de Sistemas de la Pontificia Universidad Católica del Ecuador impartir desde pregrado materias relacionadas a estándares de calidad y protección de información ya que los estudiantes necesitamos conocer desde los primeros niveles la importancia de la información y la necesidad de normas para asegurar su disponibilidad, confidencialidad e integridad.
- Se recomienda a la coordinación de maestrías en la Facultad de Ingeniería, Escuela de Sistemas de la Pontificia Universidad Católica del Ecuador implementar una materia que permita al estudiante iniciar con su Plan de Tesis previo a su egreso ya que de esa manera el estudiante recibe información oficial sobre cómo proceder con la elaboración del trabajo de Tesis, además de incentivar al estudiante a graduarse oportunamente.
- Recomendamos a nuestros compañeros maestrantes seleccionar un tema actual y de interés para el tema de su Tesis, ya que de esa manera el desarrollo de la misma fluirá con mayor velocidad. Buscar apoyo de sus docentes, director y revisores; ya que por su experiencia son de mucha ayuda a lo largo del proceso de desarrollo de la misma.

BIBLIOGRAFÍA Y REFERENCIAS

Citas, Bibliografía y Gráficos:

[A] TESIS ANÁLISIS COSTO/BENEFICIO DE LA APLICACIÓN DEL ESTÁNDAR ISO/IEC 27001:2005 A UNA EMPRESA INDUSTRIAL EN LA PROVINCIA DE PICHINCHA, Vanessa Hurtado Molina, Patricio Arias, PUCE, 2012 ABRIL.

[B] ISO/IEC 17799 Part 1: Code of practice for information security management

[C] MAGERIT, *Gestión de Riesgos de los sistemas de información, Versión 2*, ©MINISTERIO DE ADMINISTRACIONES PÚBLICAS, Madrid, 20 de junio de 2006 (v 1.1)

[D] Álvaro Soldano, *Conceptos sobre Riesgo: Síntesis temática realizada para el Foro Virtual de la RIDM creado para la Capacitación para la Teledetección Aplicada a la Reducción del Riesgo por Inundaciones*, Argentina, marzo 2009.

[E] Inteco – Deloitte, *Guía para PYMES, Cómo Implantar un Plan de Continuidad del Negocio*, 2010.

[F] Javier Areitio, *Seguridad de la Información, Redes, Informática y Sistemas de Información*, Madrid, España, Paraninfo, 2008.

[G] Robert Richardson, *15th Annual 2010/2011 Computer Crime and Security Survey*, 2011, página 15.

[H] Jeimy J. Cano, ACIS, *XI Jornada de Seguridad Informática Seguridad de la Información: Una nueva década para avanzar, III Encuesta Latinoamericana de Seguridad de la Información ACIS 2011* , 2011.

[I] Flor Nancy Díaz Piraquive, "Principales estándares para la seguridad de la información IT Alcances y consideraciones esenciales de los estándares ISO-IEC BS7799-IT, RFC2196, IT BASELINE, SSE-CMM y, ISO 27001", *Revista EOS No. 2*, Colombia, enero – abril 2008, pág 80.

[J] Estándar Internacional ISO/IEC 27001, *Tecnología de la Información – Técnicas de Seguridad – Sistemas de Gestión de Seguridad de la Información – Requerimientos*, Colombia, octubre 2005.

[K] Alejandro Corletti Estrada, *Análisis de ISO-27001:2005*, Madrid, abril de 2006, pág 1.

[L] Ramón Robles, Álvaro Rodriguez de Roa, *La gestión de la Seguridad en la empresa*, Revista Q, pág. 17, junio 2006.

[M] Ernesto R. Fontaine, *Evaluación Social de Proyectos*, Chile, 1984, Edición No. 12, página 23.

Referencias en línea:

[1] Microsoft Technet, *Guía de Administración de riesgos de seguridad*: http://www.microsoft.com/spain/technet/recursos/articulos/srsgch03.mspx Acceso: marzo 2012

[2] Drucker,Peter, *La sociedad poscapitalista*, Buenos Aires, Editorial Sudamericana. 1993

[3] Philip Kotler, Marketing Management, New Jersey, Prentice Hall, 2000, página 159.

[4] Aleida Olivé García, "La Información: Un recurso estratégico para las organizaciones", *La Revista del Empresario Cubano* , http://www.betsime.disaic.cu/secciones/tec_enemar_08.htm. Acceso: marzo 2012

[5] Novell, "European Business Communication Survey", *El Profesional de la Información: Revista Internacional Científica y Profesional*, julio 1998, Internet. http://www.elprofesionaldelainformacion.com/contenidos/1998/julio/el_uso_de_la_informacion_en_las_empresas.html Acceso: marzo 2012

[6] Arturo Grau Barberá, *Introducción a la Protección y Seguridad de la Información*, Internet. http://alarcos.inf-cr.uclm.es/doc/PSI/tema1Marian.pdf Acceso: marzo 2012

[7] Proyecto AMPARO-LACNIC, *Manual Fortalecimiento de la Capacidad Regional de Atención de Incidentes de Seguridad en América Latina y el Caribe Internet*, 2012, Internet, http://www.proyectoamparo.net/files/manual_seguridad/manual_sp.pdf, Acceso: marzo 2012

[8] CONISEC-SGSI, *Conectia-Tecnología y Comunicaciones, Propuesta de Servicios*, Internet. http://www.conisec.com/pdf/sgsi-conisec.pdf Acceso: marzo 2012

[9] David Reinares Lara, *Implantación de la ISO27001: Factores críticos de éxito y visión de la norma como motor de generación de valor añadido*, Innotec System, Internet. http://www.mundointernet.es/IMG/pdf/ponencia148_1.pdf Acceso: marzo 2012

[10] ProactivaNet, *ISO27001…¿Por dónde empezamos?,* Internet. http://www.proactivanet.com/UserFiles/File/ProactivaNET%20-%20ISO%2027001.pdf Acceso: marzo 2012

[11] International Register of ISMS Certificates, versión 212, enero 2012, Internet. http://www.iso27001certificates.com/ Acceso: marzo 2012

[12] Dejan Kosutic, *¿Cuánto cuesta la implementación de la norma ISO 27001?*, Febrero 2011, Internet. http://blog.iso27001standard.com/es/tag/iso-27001-es/, Acceso: marzo 2012

[13] Rodrigo Hiroshi Ruiz Suzuki, *"ISO 27001, la norma que define como organizar la seguridad de la información en las organizaciones"*, *Logicalis Now*, marzo 2011, Internet, http://ebookbrowse.com/ln-13-12-certificaciones-iso27001-pag-51-53-pdf-d136991637 Acceso: marzo 2012.

[14] ISO27k Implementers' Forum, Versión 3 enero 2009, Internet, http://www.iso27001security.com/ISO27k_ISMS_implementation_and_certification_process_v3.pdf, Acceso: marzo 2012

[15] "Sociedad Latinoamericana para la calidad", 2000, Internet, http://www.valoryempresa.com/archives/costobeneficio.pdf, Acceso: marzo 2012

[16] Sitio web de Adelca – Acería del Ecuador, Historia, 2011, Internet. http://www.adelca.com/sitio/esp/corporativo.php Acceso: marzo 2012

[17] AUDISEC – Retorno de inversión (ROI) en proyectos ISO 27001:2005. Alineamiento con el estándar, versión 1, 2008, Internet. http://www.angelfire.com/la2/revistalanandwan/rosintro.pdf Acceso: marzo 2012

[18] Inger Nordin, "Accreditation and certification ISMS EA Guidelines for ISMS Certification Process", 2003, Internet, http://www.docstoc.com/docs/55751922/Accreditation-and-certification-ISMS-EA-Guidelines-for-ISMS. Acceso: mayo 2012

GLOSARIO DE TERMINOS

- ACIS: Asociación Colombiana de Ingenieros de Sistemas
- Activo de información: bien tangible o intangible que representan, contienen, almacenan o transmiten información.
- ADELCA: Acería del Ecuador
- AENOR: Asociación Española de Normalización y Certificación
- AGD: Agencia de Garantía de Depósitos
- ALE: Determinación de la expectativa de pérdida anual, es la cantidad total de dinero que la empresa perderá en un año si no se toman medidas para mitigar el riesgo.
- Amenaza: es la probabilidad de ocurrencia de cualquier tipo de evento (incidente) que puede producir un daño (material o inmaterial) sobre los activos de información, en base a los principios de confidencialidad, integridad y disponibilidad de la información.
- Análisis de costo-beneficio: El análisis de costo-beneficio es una técnica importante dentro del ámbito de la teoría de la decisión. Pretende determinar la conveniencia de un proyecto mediante la enumeración y valoración posterior en términos monetarios de todos los costes y beneficios derivados directa e indirectamente de dicho proyecto.
- ARO: Determinación de la frecuencia anual, es la cantidad razonable de veces que se espera que ocurra el riesgo durante el año.
- Bot: programa informático que realiza funciones muy diversas, imitando el comportamiento de un humano.
- Bots: programa informático que realiza funciones muy diversas, imitando el comportamiento de un humano.
- BS: Estándar Británico o por sus siglas en inglés, British Standard.
- CMM: Modelo de Capacidad de Madurez
- COFIEC: Banco del Ecuador
- Competitividad: es la capacidad de generar la mayor satisfacción de los consumidores al menor precio, o sea con producción al menor costo posible.
- Confidencialidad: Garantía de la exactitud y completitud de la información y los métodos de su procesamiento.
- Control: representa todas las acciones que se implementan para prevenir la amenaza. No sólo son soluciones técnicas, sino también reflejan la capacitación y la toma de conciencia por parte de la organización, además de reglas claramente definidas.

- CSI: Computer Crime and Security
- Disponibilidad: Aseguramiento de que los usuarios autorizados tienen acceso a la información y sus activos asociados cuando lo requieran.
- Eficacia: es la capacidad de lograr un efecto deseado, esperado o anhelado
- Eficiencia: es la capacidad de lograr el efecto en cuestión con el mínimo de recursos posibles viable
- ERP: Los sistemas de planificación de recursos empresariales, o ERP (por sus siglas en inglés, Enterprise resource planning) son sistemas de información gerenciales que integran y manejan muchos de los negocios asociados con las operaciones de producción y de los aspectos de distribución de una compañía en la producción de bienes o servicios.
- Grado de Exposición: Instancia en la cual un activo de información es susceptible a dañarse por una amenaza.
- IEC: Comisión Internacional de Electrotécnica.
- Impacto: Consecuencia que produce un incidente de seguridad sobre la empresa debido a las vulnerabilidades que tiene el activo afectado.
- Incidente de Seguridad: Evento con consecuencias negativas que puede comprometer la integridad, disponibilidad y confidencialidad de la información.
- Integridad: Aseguramiento de que la información es accesible solo para aquellos autorizados a tener su acceso.
- ISO: Organización Internacional de Estándares
- IT: Information Technology por sus siglas en ingles o TI: Tecnología de la Información
- JTC1: Comités técnicos especializados No. 1
- Malware: es un tipo de software que tiene como objetivo infiltrarse o dañar una computadora sin el consentimiento de su propietario.
- Malware: es un tipo de software que tiene como objetivo infiltrarse o dañar una computadora sin el consentimiento de su propietario.
- Metodología MAGERIT[C], es un método formal para investigar los riesgos que soportan los Sistemas de Información y para recomendar las medidas apropiadas que deberían adoptarse para controlar estos riesgos.
- NIST: Instituto Nacional de Estándares y Tecnología
- OCDE: Organización para la Cooperación y el Desarrollo Económicos
- PDCA: Plan Do Check Act
- Phishing: delito encuadrado dentro del ámbito de las estafas cibernéticas
- Phising: delito encuadrado dentro del ámbito de las estafas cibernéticas

- PHVA: Planificar, Hacer, Verificar, Actuar
- OHSAS: Servicios de Consultoría de Salud Ocupacional y Seguridad
- Probabilidad de Ocurrencia: Frecuencia con la cual una amenaza puede ocurrir.
- Riesgo: Es la probabilidad de que una amenaza se convierta en un desastre aprovechando a una vulnerabilidad.
- SGI: Sistema de Gestión de Información
- SGSI: Sistema de Gestión de la Seguridad de la Información
- SLE: Determinación de la expectativa de pérdida simple, es la cantidad total de ingresos que se pierde por una única incidencia del riesgo.
- SSE-CMM: Systems Security Engineering Capability Maturity Model
- UKAS: Servicio de certificación del Reino Unido o por sus siglas en ingles, United Kingdom Accreditation Service.
- Vulnerabilidad: Conocida a veces como falencias o brechas, representa el grado de exposición a las amenazas en un contexto particular. Las vulnerabilidades están en relación directa con las amenazas, porque si no existe una amenaza, tampoco existe la vulnerabilidad o no tiene importancia, porque no se puede ocasionar un daño.

INDICE DE FIGURAS

Figura 1-01 Utilización de la Información en las Empresas[A] ……. 5

Figura 2-01 Interrelación entre variables principales que componen el riesgo[E]……. 10

Figura 2-02 Tipos de Ataques Experimentados – Por porcentaje de respuestas[G] …. 11

Figura 2-03 Tipos de Ataques Experimentados – Por porcentaje de respuestas[G]….. 12

Figura 2-04 Nivel de Participación en Seguridad de la Información - por País[H]….. 14

Figura 2-05 Presupuesto en Seguridad de la Información[H]…… 15

Figura 2-06 Incidentes de Seguridad[H]…… 16

Figura 2-07 Notificación de Incidentes de Seguridad[H]…….. 16

Figura 2-08 Políticas de Seguridad de la Información[H]……. 17

Figura 2-09 Obstáculos para Implementar la Seguridad de la Información[H]…… 18

Figura 2-10 Estándares y Buenas Prácticas de la Seguridad de la Información[G]….. 29

Figura 3-01 Razones para buscar una certificación SGSI[18]……. 31

Figura 3-02 Dominios del estándar ISO/IEC 27001[10]…… 34

Figura 3-03 Pasos para la implementación de la ISO/IEC 27001:2005[J]……. 43

Figura 5-01 Estructura Organizacional de ADELCA[A]…… 70

Figura 5-02 Proceso de Palanquillas[16]…… 72

Figura 5-03 Proceso de Laminación[16]…… 72

Figura 5-04 Proceso de Trefilación[16]……..… 73

INDICE DE CUADROS

Cuadro 2-01 Matriz de Comparación de los Estándares Presentados[I]…… 28

Cuadro 3-01 Países con número de certificaciones SGSI[11]…….…… 32

Cuadro 4-01 Descripción de Tipos de Evaluación de Riesgos[E]…….. 50

Cuadro 4-02 Clasificación de Activos[1]…… 52

Cuadro 4-03 Niveles de Defensa [1]…… 53

Cuadro 4-04 Clasificación de Activos según el impacto al negocio[1]…… 54

Cuadro 4-05 Nivel de exposición de Activos de Información [1]…… 55

Cuadro 4-06 Impacto por Clase de Activo y Nivel de Exposición[1]…….. 56

Cuadro 4-07 Probabilidad de ocurrencia del impacto[1]…….. 56

Cuadro 4-08 Nivel de Riesgo resumido[1]……..…… 57

Cuadro 4-09 Criterio para seleccionar riesgos para nivel detallado[1]…… 57

Cuadro 4-10 Primer criterio para el Nivel de Exposición, basado en la confidencialidad e integridad de la información[1]…… 59

Cuadro 4-11 Segundo criterio para calcular el Nivel de Exposición, basado en la disponibilidad de la información[1]…… 59

Cuadro 4-12 Factor de Exposición [1]…… 60

Cuadro 4-13 Nivel de Impacto Detallado [1]…… 60

Cuadro 4-14 Plantilla para el cálculo de la Probabilidad de Impacto[1]……. 62

Cuadro 4-15 Nivel de Riesgo Detallado[1]……... 63

Cuadro 4-16 Equivalencia Cualitativa Nivel de Riesgo Detallado[1]…… 63

Cuadro 4-17 Determinación de la Frecuencia Anual - ARO [1]…… 66

Cuadro 5-01 Crecimiento de la empresa en los últimos 10 años[A]…… 74

Cuadro 6-01 Descripción de activos de información que se utilizarán como referencia**[A]**…… 80

Cuadro 6-02 Clasificación de activos**[A]**…… 80

Cuadro 6-03 Identificación de incidentes de los Activos de la Información referencia**[A]** ……... 82

Cuadro 6-04 Niveles de Defensa de los activos de Referencia[A] …… 83

Cuadro 6-05 Niveles de Impacto al Negocio de los activos de referencia[A]…….. 84

Cuadro 6-06 Amenazas de los activos de referencia[A]…… 85

Cuadro 6-07 Vulnerabilidades de los activos de referencia[A]…… 87

Cuadro 6-08 Nivel de exposición de los activos de referencia[A]…… 88

Cuadro 6-09 Impacto del activo de referencia AI1.1[1]……..... 89

Cuadro 6-10 Impacto del activo de referencia AI25.1[1]…….. 90

Cuadro 6-11 Impacto del activo de referencia AI25.2[1]…….. 90

Cuadro 6-12 Nivel de riesgo resumido del activo de referencia AI1.1[1]…… 92

Cuadro 6-13 Nivel de riesgo resumido del activo de referencia AI25.1[1]……... 92

Cuadro 6-14 Nivel de riesgo resumido del activo de referencia AI25.2[1]……... 93

Cuadro 6-15 Lista resumida de riesgos del activo de información utilizado como referencia[A]…… 93

Cuadro 6-16 Lista de activos para nivel de riesgo detallado[A]…… 96

Cuadro 6-17 Controles propuestos para los activos de referencia Anexo A de la ISO/IEC 27002:2005[A]……... 97

Cuadro 6-18 Nivel de exposición detallado sin la ISO/IEC 27001:2005[A]……. 99

Cuadro 6-19 Nivel de exposición detallado con la ISO/IEC 27001:2005[A]…… 99

Cuadro 6-20 Nivel de impacto detallado sin la ISO/IEC 27001:2005[A]……. 100

Cuadro 6-21 Nivel de impacto detallado con la ISO/IEC 27001:2005[A]…… 101

Cuadro 6-22 Probabilidad de impacto detallado[A]…….. 103

Cuadro 6-23 Nivel de riesgo detallado sin ISO/IEC 27001:2005[1]…… 104

Cuadro 6-24 Nivel de riesgo detallado con ISO/IEC 27001:2005[1]…… 105

Cuadro 6-25 Categorización de activos para determinar los valores directos e indirectos[A]……. 106

Cuadro 6-26 Asignación de Valor Directo a activos utilizados como referencia[A]. 107

Cuadro 6-27 Asignación de Valor Indirecto al activo utilizado como referencia[A] 107

Cuadro 6-28 Cuantificación del activo utilizado como referencia[A]……... 109

Cuadro 6-29 Valoración por clase de activo de Impacto al Negocio[A]……... 110

Cuadro 6-30 Valoración por clase de activo de Impacto al Negocio sin ISO/IEC 27001:2005[A]…….… 112

Cuadro 6-31 Valoración por clase de activo de Impacto al Negocio con ISO/IEC 27001:2005[A]..... 112

Cuadro 6-32 Comparativo del riesgo sin control y con control por activo[A]…….. 113

Cuadro 6-33 Expectativa de pérdida simple y anual sin ISO/IEC 27001:2005[A]... 113

Cuadro 6-34 Expectativa de pérdida simple y anual con ISO/IEC 27001:2005[A].. 113

Cuadro 6-35 Resumen costos de implementación ISO/IEC 27001[A]…… 114

Cuadro 6-36 Cálculo de ROSI[A]……. 115

Cuadro 6-37 Relación de Inversión[A]…….. 115

Cuadro 6-38 Relación de riesgo disminuido sobre riesgo inicial[A]……. 116

Cuadro 6-39 Relación Beneficio sobre el riesgo[A]…….. 116

Cuadro 6-40 Relación de Inversión respecto al riesgo[A]……. 116

INDICE DE ANEXOS

ANEXO A: Síntesis del estándar ISO/IEC 27001:2005[J]

ANEXO B: Implementación de la ISO/IEC 27001:2005[J]

ANEXO C: Descripción y clasificación de los Activos de la Empresa e identificación de incidentes relacionados [1]

ANEXO D: Nivel de Defensa, Clase de Activos por Impacto al Negocio, Amenazas, Vulnerabilidades y Nivel de Exposición de los Activos de Información de la Empresa[1]

ANEXO E: Lista Resumida de Riesgos por Activos de Información[1]……

ANEXO F-01: Lista de Prioridades de Riesgos Detallado por Activos de Información – Situación Actual[1]……...

ANEXO F-02: Lista de Prioridades de Riesgos Detallado por Activos de Información – Situación Proyectada[1]……

ANEXO G: Cuantificación de Activos[1].....

ANEXO H-01: Expectativa de Pérdida Anual – Situación Actual[1]…….

ANEXO H-02: Expectativa de Pérdida Anual – Situación Proyectada[1]……..

ANEXO I: Costos de los Controles a implementar en la empresa…….