



UNIVERSIDAD JUÁREZ AUTÓNOMA DE TABASCO

DIVISIÓN ACADÉMICA DE INFORMÁTICA Y SISTEMAS



**MODELO DE ANÁLISIS PARA LA PREVENCIÓN DE
RIESGOS EN LA SEGURIDAD DE INFORMACIÓN. CASO:
E&B PROMOCIÓN EMPRESARIAL S.A. DE C.V.**

Trabajo recepcional bajo la modalidad de Tesis

Que para obtener el grado de:

Maestro en Administración de Tecnologías de la Información

Presenta:

Ing. José Manuel Torres Hernández

Director:

Dr. José Adán Hernández Nolasco

Cuerpo Académico:

Sistemas Distribuidos

Líneas de generación y aplicación del conocimiento:

Sistemas Distribuidos

Sistemas de Comunicación

Cunduacán, Tabasco

Diciembre, 2012



UNIVERSIDAD JUÁREZ AUTÓNOMA DE TABASCO

DIVISIÓN ACADÉMICA DE INFORMÁTICA Y SISTEMAS



**MODELO DE ANÁLISIS PARA LA PREVENCIÓN DE
RIESGOS EN LA SEGURIDAD DE INFORMACIÓN. CASO:
E&B PROMOCIÓN EMPRESARIAL S.A. DE C.V.**

Trabajo recepcional bajo la modalidad de Tesis

Que para obtener el grado de:

Maestro en Administración de Tecnologías de la Información

Presenta:

Ing. José Manuel Torres Hernández.

Director:

Dr. José Adán Hernández Nolasco.

Revisores:

Dr. Miguel Antonio Wister Ovando.

M.C. Pablo Pancardo García.

M.I. Héctor Toraya Lazo de la Vega.

Cunduacán, Tabasco

Diciembre, 2012



UNIVERSIDAD JUÁREZ AUTÓNOMA DE TABASCO

"ESTUDIO EN LA DUDA. ACCIÓN EN LA FE"

DIVISIÓN ACADÉMICA DE INFORMÁTICA Y SISTEMAS



Oficio No.2943/12/DAIS/D
Diciembre 10 de 2012

ING. JOSÉ MANUEL TORRES HERNÁNDEZ
PRESENTE

En virtud de que cumple satisfactoriamente los requisitos establecidos en el Reglamento de Estudios de Posgrado vigente en la Universidad, informo a Usted que se autoriza la impresión del trabajo de investigación **"Modelo de análisis para la prevención de riesgos en la seguridad de información. Caso E&B Promoción Empresarial, S.A. de C.V."**, para presentar Examen de Grado de la Maestría en Administración de Tecnologías de la Información, bajo la modalidad de Tesis.

Sin otro particular, aprovecho la ocasión para enviarle un afectuoso saludo.

Atentamente

Lic. Eduardo Cruces Gutiérrez
Director

c.c.p. Lic. Martha Patricia Silva Payró.- Coordinadora de Investigación y Posgrado.
Archivo.
Consecutivo.



Universidad Juárez Autónoma de Tabasco

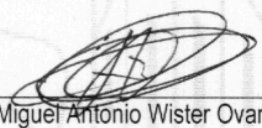
"Estudio en la duda, acción en la fe"

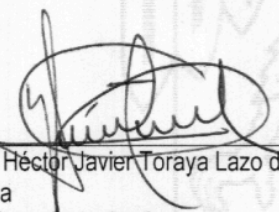
División Académica de Informática y Sistemas

En la Universidad Juárez Autónoma de Tabasco, de acuerdo al Reglamento de Estudios de Posgrado vigente, se revisó el trabajo de investigación titulado "Modelo de análisis para la prevención de riesgos en la seguridad de información. Caso E&B Promoción Empresarial, S.A. de C.V.", realizado por el C. José Manuel Torres Hernández, para obtener el Grado de Maestro en Administración de Tecnologías de la Información bajo la modalidad de Tesis.

Los integrantes del jurado, después de revisar el trabajo, lo declararon aceptado.


M.C. Pablo Páncardo García
Profesor-Investigador


Dr. Miguel Antonio Wister Ovando
Profesor-Investigador


M.I. Héctor Javier Toraya Lazo de la
Vega
Profesor-Investigador

Carta de Autorizacion

A quien corresponda:

El que suscribe, autoriza por medio del presente escrito a la Universidad Juárez Autónoma de Tabasco para que utilice tanto física como digitalmente la tesis de grado denominada, **“Modelo de análisis para la prevención de riesgos en la seguridad de información. Caso: E&B Promoción Empresarial S.A. de C.V”**, de la cual soy autor y titular de los Derechos de Autor.

La finalidad del uso por parte de la Universidad Juárez Autónoma de Tabasco de la tesis antes mencionada, será única y exclusivamente para difusión, educación y sin fines de lucro; autorización que se hace de manera enunciativa mas no limitativa para subirla a la Red Abierta de Bibliotecas Digitales (RABID) y a cualquier otra red académica con las que la Universidad tenga relación institucional.

Por lo antes manifestado, libero a la Universidad Juárez Autónoma de Tabasco de cualquier reclamación legal que pudiera ejercer respecto al uso y manipulación de la tesis mencionada y para los fines estipulados en este documento.

Se firma la presente autorización en la ciudad de Villahermosa, Tabasco a los 11 días del mes de Diciembre del 20012.

Autorizo



Ing. José Manuel Torres Hernández.



UNIVERSIDAD JUÁREZ AUTÓNOMA DE TABASCO

"ESTUDIO EN LA DUDA. ACCIÓN EN LA FE"

DIVISIÓN ACADÉMICA DE INFORMÁTICA Y SISTEMAS



Oficio No. 2362/12/DAIS/D
Septiembre 20 de 2012

Dr. José Adán Hernández Nolasco
Profesor-Investigador
Presente

De acuerdo al artículo 44 fracción 3 del Reglamento de Estudios de Posgrado, de la Universidad Juárez Autónoma de Tabasco, me permito informar a Usted, que ha sido designado Director del trabajo de Tesis titulado **"Modelo de análisis para la prevención de riesgos en la seguridad de información. Caso E&B Promoción Empresarial S.A. de C.V."**, a realizar por el **C. José Manuel Torres Hernández**, para obtener el grado de Maestro en Administración de Tecnologías de la Información.

Sin otro particular, aprovecho la ocasión para enviarle un afectuoso saludo.

Atentamente


Lic. Eduardo Cruces Gutiérrez
Director

c.c.p. Lic. Martha Patricia Silva Payró.- Coordinadora de Investigación y Posgrado.
Archivo.
Consecutivo.



Dedicatoria

La culminación de este proyecto va dedicada para aquellas personas que me han brindado su confianza y apoyo incondicional durante esta etapa de mi formación profesional.

A Dios.

Por su bondad al iluminarme en tiempos de flaqueza y darme el espíritu de superación, entrega y pasión por las cosas que realizo.

A mis padres.

Por ser ejemplo de unión, amor, entrega, confianza y su comprensión; por brindarme aquellos valores que me han ayudado a forjarme como persona. Ambos, les doy infinitamente las gracias por sus enseñanzas y apoyo, ya que han sido mi pilar y guía constante en todo lo que realizo.

A la Lic. Ana María

Porque su presencia ha sido principal fuente de motivación para la elección del tema y soporte en la toma de decisiones.

Agradecimientos

De manera cordial y afectuosa quiero agradecer a mi asesor el *M.C. Jose Adán Hernández Nolasco* por sus consejos, tiempo y siempre certeras contribuciones para hacer posible la culminación de este proyecto.

Además a quienes con sus anotación hicieron posible el mejoramiento de este trabajo, mis revisores de tesis: *Dr. Miguel Antonio Wister Ovando, M.C. Pablo Pancardo García y el M.I. Héctor Toraya Lazo de la Vega*, les agradezco por sus valiosas aportaciones.

Así también a nuestra máxima casa de estudio la *Universidad Juárez Autónoma de Tabasco* y en especial a la *División Académica de Informática y Sistemas* por su apoyo y atenciones prestadas durante la realización de mi proyecto y en general del posgrado.

Y desde luego no puedo dejar de mencionar a las autoridades universitarias que estuvieron a cargo y quien además mostraron su dedicación, apoyo y entusiasmo para que concluyera con éxito el posgrado, la *Lic. Martha Patricia Silva Payró y el Lic. Eduardo Cruces Gutiérrez*.

Tabla de contenido

Tabla de contenido	10
Índice de Ilustraciones.....	12
Índice de Tablas	13
Resumen	15
Introducción	16
Capítulo I. Generalidades.....	17
1.1 Antecedentes	17
1.2 Planteamiento del problema	21
1.2.1 Definición del problema.....	21
1.3 Objetivo general	23
1.3.1 Objetivos específicos.....	23
1.4 Justificación.....	23
1.5 Delimitación de la investigación	26
1.5.1 Alcances	26
1.5.2 Limitaciones.....	26
1.6 Metodología utilizada.....	26
1.6.1 Metodología de la investigación	28
Capítulo II. Marco Teórico.....	33
2.1 Marco conceptual	33
2.1.1 Inteligencia competitiva	33
2.1.2 Contrainteligencia empresarial.....	33
2.1.3 Activos	35
2.1.4 Dato	35
2.1.5 Conocimiento	36
2.1.6 Información	36
2.1.7 Insiders	40
2.1.8 Seguridad de la información	41

2.1.9 Delito informático	44
2.1.10 Ataques informáticos.....	45
2.1.11 Políticas de seguridad.....	47
2.1.12 Amenazas	49
2.1.13 Riesgos.....	50
2.1.14 Impacto.....	51
2.1.15 DLP	52
2.1.16 Método MAGERIT	52
2.1.17 Análisis de riesgos.....	53
2.1.18 MEHARI.....	55
2.1.19 Métrica V3.....	55
2.1.20 Valores porcentuales	55
Capítulo III. Aplicación de la metodología y desarrollo.....	57
Capítulo IV. Pruebas y Resultados.....	70
Capítulo V. Conclusiones y trabajos futuros.....	89
5.1 Conclusiones	89
5.2 Trabajos futuros.....	90
Capítulo VI. Bibliografía.....	92
Glosario	98
Anexos y Apéndices.....	99

Índice de Ilustraciones.

Ilustración 1 Metodología a utilizar	29
Ilustración 2 Ciclo contrainteligencia	34
Ilustración 3 Distribución de la empresa.....	65
Ilustración 4 Gráfica de la susceptibilidad del activo.	77
Ilustración 5 Gráfica de los niveles porcentuales según el tipo de riesgo	78
Ilustración 6 Gráfica del porcentaje de impacto en los activos.....	85
Ilustración 7 Gráfica de las amenazas según su impacto	86

Índice de Tablas

Tabla 1 Objetivo de las metodologías.....	58
Tabla 2 Elementos principales de las metodologías.....	59
Tabla 3 Comparativa de las fases.....	59
Tabla 4 Aplicaciones informáticas.....	63
Tabla 5 Infomercados según su enfoque.....	64
Tabla 6 Aplicaciones informáticas según el personal.....	65
Tabla 7 Frecuencia de amenazas.....	68
Tabla 7. a) Servicios de promoción directa.....	71
Tabla 7. b) Servicios de promoción de Unilever.....	71
Tabla 7. c) Servicios de apoyo promocional y alianzas estratégicas.....	72
Tabla 7. d) Administración de personal y aplicaciones informáticas (Software).....	72
Tabla 7. e) Aplicaciones informáticas: Infomercados externo.....	73
Tabla 7. f) Aplicaciones informáticas: Infomercados Interno.....	73
Tabla 7. g) Equipos informáticos (hardware), instalaciones y redes de comunicaciones.....	74
Tabla 8 Impacto de las amenazas.....	69
Tabla 8. a) Servicios de promoción directa.....	79
Tabla 8. b) Servicios de promoción Unilever.....	79
Tabla 8. c) Servicios de eventos y edecanes.....	80
Tabla 8. d) Servicios de apoyo promocional y alianzas estratégicas.....	80
Tabla 8. e) Aplicaciones informáticas.....	81
Tabla 8. f) Aplicaciones informáticas: Infomercados externo.....	81
Tabla 8. g) Aplicaciones informáticas: Infomercados interno.....	82
Tabla 8. h) Equipos informáticos (hardware), instalaciones y redes de comunicaciones.....	82
Tabla 9 Concentrado general de frecuencia de amenazas.....	75
Tabla 10 Evaluación de la susceptibilidad de los activos.....	76
Tabla 11 Concentrado general del impacto del riesgo.....	83

Tabla 12 Evaluación de las amenazas que impactan a los activos.....	84
Tabla 13 Compendio de la frecuencia de los riesgos	87
Tabla 14 Compendio del impacto de riesgos	88

Universidad Juárez Autónoma de Tabasco.
México.

Resumen

En esta investigación se presenta un estudio que permite resaltar la importancia en la seguridad de los sistemas información, teniendo como propósito concientizar sobre el resguardo del activo más importante que es la información, enfocando específicamente a la empresa E&B Promoción Empresarial que se analiza a lo largo del estudio.

Ahora bien, para una mejor comprensión en el cumplimiento del objetivo de este trabajo se analizaron los riesgos que usualmente se presentan en las organizaciones que afectan a la seguridad de la información y se propone el uso de modelos de análisis de riesgos para la prevención de pérdida de información que mejor se adecuen al caso de estudio en particular.

Específicamente, el proyecto ha consistido en la realización de un análisis de riesgos de seguridad de la información que permita cuantificar y comparar los requerimientos de seguridad de la información de la organización con los controles implantados para su cumplimiento, y, en base a las diferencias encontradas, definir los controles adicionales necesarios para cumplir todos los requerimientos para así evitar futuras pérdidas o brechas que podrían derivar situaciones críticas que impacten la vida de la empresa.

A lo largo del desarrollo de esta investigación, ⁵ primero, se utilizaron técnicas cualitativas para comprender en su totalidad el fenómeno, logrando así una visión más amplia de los aspectos globales de la empresa, a partir de esta primera incursión se refinaron las preguntas de investigación y finalmente se formuló la hipótesis. No obstante, en la fase de recolección de datos para el análisis, se utilizaron técnicas de ambos enfoques, uno que profundizar en el conocimiento de las áreas de oportunidad y el otro que logra la precisión en los datos que permiten plantear conclusiones y generalizaciones.

Introducción

La información, en todas sus formas es uno de los principales activos de cualquier organización, necesaria para el normal funcionamiento y la consecución de los objetivos que tenga marcados.

Debido a esa importancia, las organizaciones necesitan proteger su información para asegurar que esté disponible cuando se necesite, que sea fiable y que su distribución esté controlada. Esta necesidad se ve agravada por el hecho de que la cantidad de información que maneja una organización y su complejidad crece de forma exponencial, dificultando los esfuerzos para su protección (management, 2008).

Es por lo anterior que se presenta una propuesta basada en un modelo de análisis de riesgo para la seguridad de la información, lo cual se expone a través de cinco capítulos que se describen a continuación.

En el primer capítulo de generalidades se describe el planteamiento del problema, los objetivos justificación y delimitación de este proyecto, ya que es importante analizar la problemática para poder desarrollar una solución adecuada.

La explicación de conceptos fundamentales, así como los requerimientos legales, normativos, y el estado del arte se describen en el capítulo II. Ya que se debe conocer el tema a desarrollar. En el tercer capítulo se exponen las herramientas para obtener la información sobre el tema de estudio y de las soluciones que se proponen de acuerdo a la metodología seleccionada.

El capítulo IV presenta el desarrollo de la solución óptima seleccionada, describiendo las herramientas usadas, requerimientos físicos y tecnológicos de acuerdo al proyecto de investigacio. Finalmente, en el capítulo V, con la información recolectada y desarrollada se presentan las diversas conclusiones a las que se llegó, así como los trabajos futuros, es decir, aquellos que parten del estudio que en este proyecto se presenta.

Capítulo I. Generalidades

1.1 Antecedentes

En la actualidad las personas cuentan con la facilidad en el manejo de dispositivos electrónicos, encargados de manipular y almacenar la información, esto es debido a que se han tornado necesarias para un mejor desempeño en sus labores diarias. Es de notar que las tecnologías de la información evolucionan con una velocidad vertiginosa, lo cual genera interés por asegurar sus activos y reforzar en cuanto a seguridad se refiere (FIA, 2007).

Comencemos por mencionar que el personal encargado del área de sistemas no solo es el responsable en el manejo de la información, también existen agentes externos en su manipulación. Lo anterior lo aclara en una entrevista realizada por Borghello al director de Cybsec S.A. Security System Julio C. Ardita, explica que "(...) desde mitad de 1996 hasta 1999 la empresa tuvo dos casos de intrusiones, pero en el 2000 registramos siete, de las cuales 5 eran intrusos internos o ex-empleados (...)". Cristian F. Borghello aclara que esto es realmente preocupante, por que, una persona que trabaje ya sea con el administrador, el programador o el encargado de una máquina conocen perfectamente como trabaja el sistema, sus puntos fuertes y débiles; de manera que un ataque realizado por esa persona podrá ser más directo, difícil de detectar y más efectivo que el que un atacante externo pueda realizar (Borghello C. F., 2009).

En este sentido es bueno mencionar que el término de contrainteligencia empresarial se usa como herramienta de sustentación de ventajas competitivas, donde en el manejo de la inteligencia competitiva tiene un nuevo papel en la vida de las empresas porque utiliza la información como su recurso (Cardoso Jr, 2007). Esto conduce a ubicarnos en el argumento de como el mundo empresarial toma un giro con la era del conocimiento, donde el activo de la información es de suma importancia y entra en el ambiente competitivo. Es decir, que no solo se debe preocupar de las amenazas de los hackers, si no también de las personas que cuentan con información

confidencial por razón de su cargo (conocidos como insiders en adelante).

Y aunque se hacen esfuerzos en materia de seguridad dentro de las empresas, no es simple coincidencia que estas sean insuficientes. Sin embargo, no hay que dejar pasar por alto ningún detalle ya que las pérdidas siguen presentándose. Es por eso que se observa como las organizaciones particulares y gubernamentales cuentan aparentemente con una estructura firme pero sin estar exentas de fugas o fallas en su personal (Pacheco, 2011).

Con todo y lo anterior, es bueno señalar que existe una infinidad de casos alrededor del mundo. A continuación se enfatizan empresas que han reportado severos problemas debido al manejo incorrecto de información, donde han registrado brechas que por lo general se reflejan comúnmente en pérdidas económicas, por citar algunos ejemplos tenemos:

En el 2007 las carreras de la fórmula 1 con la escudería Ferrari se vio afectado por espionaje, cuando una tienda de fotocopias tomo datos importantes sobre uno de sus vehículos para poder realizar un sabotaje y perjudicar la carrera en Mónaco por parte de la escudería McLaren (Ediciones El pais S.L., 2007); En diciembre del 2009 la red social Tuenti fue afectada por el robo de 4000 cuentas de usuarios y sus contraseñas, por parte de un atacante enojado con la empresa (Pacheco, 2011); El caso wikileaks uno de los ejemplos más controversiales mediáticamente, ocurridos en el 2010 donde se fugaron más de 260 mil informes y cables de agencias de gobierno debido a un mal manejo de la información del personal que en su momento pudo manipular, transformándose en la mayor filtración de documentos secretos de la historia según el gerente de investigación y educación de ESET (Bortnik, 2010).

Por otra parte, en cuanto a empresas Mexicanas que han empleado algunas de las metodologías en el análisis de riesgos dedicadas a la seguridad de la información se encuentra Deloitte Consulting Group, S.C., dedicada a la auditoría, impuestos, consultoría y asesoría financiera en ese momento realizadas a grupo modelo. También la empresa AENOR México brinda servicio global de análisis a los clientes del sector agroalimentario y ha implementado MAGERIT para su análisis en algunos de sus casos (AENOR , 2003).

Con todo esto en mente los expertos en el tema han realizado estudios y planteado una serie de metodologías para el análisis de riesgos de información. Por mencionar algunas, basándose en lo considerable del beneficio hacia las empresas tenemos:

La Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (MAGERIT en adelante): da a conocer el riesgo al que están sometidos los elementos de trabajo, utiliza aproximaciones metódicas y herramientas de soporte las cuales buscan objetivar el análisis para saber el grado de seguridad (Ministerio de administraciones públicas, 2006).

El método de análisis de riesgo armonizado (MEHARI en adelante por sus siglas en francés): incluye, directamente en las bases de conocimiento, las fórmulas del método para la evaluación directa de los riesgos y la valoración de las formas de tratar y reducir los mismos (MEHARI, 2010).

Y la métrica versión 3: Instrumento útil para la sistematización de las actividades que dan soporte al ciclo de vida del software actualmente están conviviendo y los aspectos de gestión que aseguran que un proyecto cumple sus objetivos en términos de calidad, coste y plazos. (Pechuan, 1996).

Por otra parte, de acuerdo con el análisis del BSA (Business Software Alliance por sus siglas en inglés) México posee un índice por arriba del 55% en delitos relacionados con la seguridad de la información. Los principales delitos que se destacan son los fraudes, la falsificación y la venta de la información (Business Software Alliance, 2010).

Al margen de lo anterior el profesor de inteligencia empresarial estratégica en el master en administración de la UNISUL Walter Félix, en una entrevista asevera lo siguiente: “Cualquier insumo informacional puede ser obtenido sin la autorización, ayuda o el conocimiento de persona u organizaciones. Es un mundo comandado por la inteligencia de los negocios, eso hace las cuestiones de seguridad aun más complicadas.” (Cardoso Jr, 2007). Con base a esto se destaca

que los casos por pérdida de datos en la gran mayoría son producidos por empleados, gerentes, líderes o consultores con información privilegiada; Personal que por su trabajo se ven en la necesidad de manejar datos sensibles como finanzas, base de datos, propiedad intelectual u otra información confidencial; Violando políticas de la empresa y exigencias de regulación.

Aún así la empresa S2 Grupo especializada en la seguridad de los procesos de negocio describe en un artículo de su página presentado por Patricia Vanaclocha titulado “Errores comunes en la implantación de un Sistema de Gestión de la Seguridad de la Información (SGSI en adelante)”, donde en síntesis aclara que el SGSI no solo es un trámite laboral si no que se tiene que mantener, dado que es un sistema de mejora continua y el entorno en el que se desarrolla cambia. Enfatizando que el equipo de informática no es el total responsable de la seguridad de la información (Vanaclocha, 2009).

Para los fines de nuestro argumento cabe señalar que la empresa E&B promoción empresarial, no se encuentra exenta de estos casos. Conviene distinguir que es una empresa dedicada a promover marcas en el mercado, la cual sufrió pérdidas monetarias en la ruptura de acuerdos comerciales con el Banco BBVA por fuga de información realizadas por uno de sus ejecutivos en Abril 2011. Estos hechos muestran que los componentes del sistema de información no cuentan con un adecuado nivel de seguridad o madurez en el manejo de la información, lo cual es un detonante mostrando una debilidad que por consiguiente se podrá inducir a un espionaje empresarial o una competencia desleal.

Actualmente este tipo de practicas surgen con mayor frecuencia siempre teniendo como base el lucro de la información para obtener algo un beneficio, llevando así a la empresa usurpada a un escenario critico. Es importante mencionar que el modelo de análisis para la prevención de riesgos en la seguridad de la información basa su funcionamiento en métodos y procedimientos que pueden ser implementados en cualquier empresa sin importar el tipo de giro que pertenezca.

Derivado de dicha situación, se considera importante indagar en una solución por prever estos errores, mostrando la vulnerabilidad a la que está expuesta la organización, demostrando que toda

la información puede ser extraída por un descuido o conscientemente, causando problemas tanto financieros como de operación.

1.2 Planteamiento del problema

1.2.1 Definición del problema

³ En los últimos años, la materia de seguridad de la información ha tenido un rápido crecimiento generada por la urgencia de formalizar las medidas de seguridad necesarias para resguardar la información. De esta forma, el tema de la seguridad basado en la tecnología ha pasado a un aspecto de seguridad más global.

De manera que las empresas con problemas de seguridad en sus sistemas de información son cada vez más habituales. Esto se debe a que existe un fuerte entorno competitivo y globalizado, donde las organizaciones se ven en la necesidad de volverse dependientes en las áreas tecnológicas y administrativas para poder llevar a cabo su operativa. Este argumento corresponde bien al suceso que la promotora de servicios E&B vivió y al igual que otras empresas alrededor del mundo han tenido pérdidas o fugas en sus sistemas de información. Añádase que dependiendo de la magnitud del riesgo en la información se verán obligados a decidir si sigue o no la empresa según los daños que repercute.

¹² Las áreas de informática hoy en día cuentan con jefes de seguridad y administradores de TI que deben dotarse constantemente de innumerables y eficientes herramientas de protección de información, para así proporcionar soluciones de seguridad. Sin embargo, los hackers o insiders según sea el caso, continúan atacando sus sistemas y robando contenidos valiosos. Esto nos lleva al punto inicial del problema que surge en la empresa E&B, encendiendo un foco rojo, ya que siguen reportando que las bases de datos son vulnerables en cuanto seguridad se refiere, admitamos que el problema que genera mayor preocupación es que persisten las ventilaciones de documentos de carácter confidencial.

Conviene distinguir que las filtraciones realizadas deben ser sometidas a un minucioso análisis para evitar que se sigan produciendo, a tal grado que estas resulten como consecuencias severas pérdidas de tiempo, dinero y de la información, no obstante hablamos de pérdidas considerables para la empresa ya que afecta directamente en su desempeño, por consiguiente crea una fractura organizacional al no saber en dónde se originó tal fuga.

Lo que nos lleva a advertir que la pérdida de registros confidenciales está generando un grave impacto en las finanzas y en la imagen de las organizaciones, donde empresas transnacionales e incluso gobiernos de los países están siendo afectadas, por consiguiente se esta detonando un problema global. México no se encuentra libre de brechas de información puesto que el costo de las pérdidas de datos también está escalando, con numerosos casos de multas y demandas que provocan pérdida de millones de pesos (Mistretta, 2009).

Estas consideraciones fundamentan mi propuesta de que es necesario reformar estrategias de seguridad y confidencialidad en las áreas de informática con una adecuada participación de todos los colaboradores, mediante una comunicación efectiva y una planeación apropiada donde la empresa considere la participación todo el personal. No cabe duda que el alcance del problema por pérdida de información es proporcional a la magnitud de la protección brindada hacia elementos externos, a lo cual este estudio hace hincapié en errores comunes que pueden ser catastróficos para E&B al igual que para cualquier empresa.

De lo anterior expuesto se formulan las siguientes preguntas de investigación:

- ¿Que características en el manejo de la información permite definir un modelo apropiado para garantizar la seguridad de la información de la empresa E&B promoción empresarial?
- ¿Cuáles son las fallas de seguridad de la información más frecuentes en cuanto a pérdida de datos?
- ¿Qué relación existe entre los aspectos tecnológicos, humanos-sociales y administrativos en cuanto a seguridad de la información de la empresa?

1.3 Objetivo general

Analizar y detectar los riesgos de seguridad en la información para la empresa E&B, que permita proponer e implementar un modelo apropiado con los controles, procedimientos y herramientas para la prevención de pérdida de información, apoyándose del ciclo de contra-inteligencia.

1.3.1 Objetivos específicos

- Identificar y diferenciar los controles, políticas y procesos de seguridad para reconocer el grado de confiabilidad en el análisis de riesgos de E&B promoción empresarial S.A. de C.V.
- Analizar y seleccionar los elementos de las metodologías de análisis de riesgos (MAGERIT, MAHERIT, y métrica V3) y ver la que mejor se adecue a la empresa E&B.
- Implementar y adecuar una metodología en E&B promoción empresarial S.A. de C.V.
- Evaluar el modelo en relación al personal, su capacidad de manipulación de contenidos y los controles de seguridad existentes en la infraestructura de TI en E&B promoción empresarial S.A. de C.V.
- Revisar y evaluar con las nuevas políticas de seguridad la organización: roles, responsabilidades y su estructura.
- Definir la política de seguridad y establecer el alcance del SGSI (Sistema de Gestión de Seguridad de información).

1.4 Justificación

En la actualidad se tiene la idea que el manejo de la información y los procedimientos de control de seguridad es responsabilidad del personal del departamento de Sistemas/Informática, pero se debe cambiar este paradigma para reconocer que estas son responsabilidades conjuntas de los usuarios, del departamento de control interno y de sistemas, por eso es importante tomar en cuenta todo los recursos que se tienen a la mano que permiten detectar las deficiencias.

De igual modo existen protocolos de seguridad de información que son claves para generar un alto rendimiento, por lo tanto estos deben estar en constante monitoreo y así evitar todo tipo de complicaciones, al respecto conviene decir que la prevención de pérdida de datos es una solución imprescindible para las organizaciones actuales. De ahí que el personal encargado de las decisiones importantes debe buscar a gente especializada con amplia experiencia en análisis de contenido que sepa seleccionar la solución de su clase.

La importancia de este estudio es evidenciar las áreas de oportunidad para generar conciencia de todo lo que se está dejando a un lado como es la seguridad en el manejo de la información y así obtener un mejor control del valor más importante de la empresa.

Ahora bien, el uso del método de análisis y gestión de riesgos de los sistemas de información prepara a la organización para procesos de evaluación mediante un modelo sistemático en el análisis de áreas de oportunidad, que permite mantener los riesgos bajo control por lo tanto ayudan a descubrir y planificar las medidas oportunas. De estas circunstancias nace el hecho que planteando un ordenado estatuto se tiene que apegar cada uno de los colaboradores, a pesar de todo, este método no elimina el cien por ciento los problemas de seguridad pero sí establece una valoración de los riesgos a los que se enfrenta la organización en materia de la información.

Dentro de este marco se debe considerar que al definir las políticas que regulen a E&B promoción empresarial S.A. de C.V. servirá para el oportuno manejo de la información. Entonces resulta que generando así ⁴ una planificación de las actividades defensivas como un todo, ciertamente pasando por la evaluación de la competencia y de los puntos vulnerables de la propia organización, así como por el desarrollo y aplicación de las contramedidas recomendables, se llega al procesamiento (que incluye actividades de análisis especializado) y la diseminación selectiva de informaciones volcadas a la contra-inteligencia. Llegado a este punto es bueno mencionar que los procesos de colecta externa y los servicios internos de protección de las informaciones sensibles pueden ser integrados en un mismo modelo en el contexto de la gestión estratégica de la organización (Miller, 2002)

Es así como considerando los grandes esfuerzos por proteger las redes de información se han creado: sistemas de prevención de intrusos (que escanean paquetes de contenido potencialmente dañinos), sistemas de seguridad que analizan virus de e-mail (contengan conexiones no solicitadas o bloqueadas), sistemas para detener los ataques de las amenazas de redes corporativas y gubernamentales. En general, estas aplicaciones de prevención de seguridad vienen haciendo un trabajo bastante efectivo pero deficiente cuando se habla de una intrusión no autorizada por el personal con ciertos privilegios.

Con el fin de encontrar en E&B promoción empresarial S.A. de C.V. la razón de las fugas de información y generar interés a los jefes por proteger su activo más valioso, descubriendo los errores que se generan en el manejo de la información por parte de los empleados. Se busca dentro un grupo seleccionado de metodologías de análisis de riesgos el estudio del caso y generar un nuevo conocimiento en la empresa para saber en qué parte de la estructura de la organización se encuentran controles de seguridad débiles y así poder fortalecerlos.

De lo anterior se puede entender observando las tres metodologías que se analizan, estas son: la MAGERIT, MEHARI, y la métrica V3. No se trata tan solo de metodologías, ya que plantean modelos capaces de dotar a las empresas de una cultura de prevención de riesgos que plasman la gestión oportuna de los problemas vinculados con la seguridad de la información. Estas se analizarán y detallarán para adecuarlas a las áreas de oportunidad que se quieren definir buscando un óptimo resultado.

Enfatizando, las metodologías describen que la seguridad de la información debe ser gestionada como un proceso, no sólo abarcando temas tecnológicos, sino aspectos que comienzan desde la propia gestión en las personas.

Cabe señalar que un punto importante en la elaboración de este proyecto es que a pesar de que E&B promoción empresarial, empresa a la que se le realiza el estudio es una promotora y

administradora de recursos humanos, el estudio se puede aplicar en otros sectores de la industria en otros ramos, siempre y cuando se quiera mejorar su estructura de seguridad.

1.5 Delimitación de la investigación

1.5.1 Alcances

Detección y reducción de las fugas de información, focalizando y reparando las brechas que se presenten, e implementar de tres metodologías, la que se adecue en el análisis de riesgos de E&B Promoción Empresarial S.A. de C.V. proporcionando una visión integral al problema, asegurando las áreas de oportunidad que en último término descompensarían y consecuentemente, harían ineficaz el sistema de gestión.

1.5.2 Limitaciones.

- Entre las restricciones que se presentan son: las normas que presiden, el carácter del contrato y la confidencialidad a la que se obligue la empresa restringiendo el acceso a cierta información. Por dichas razones, no se podrá implementar limitando el proyecto únicamente a la propuesta de solución de seguridad.
- En este trabajo únicamente se consideraron solo las metodologías: MAGERIT , MEHARI y la métrica V3.

1.6 Metodología utilizada

El presente estudio se insertó en un enfoque **mixto**, ya que el enfoque **cuantitativo** y el **cualitativo** tienen varios aspectos en común. En el cuantitativo por la recolección y análisis de datos probó las hipótesis que fueron formuladas previamente. Enfatizo el análisis de partes o componentes de los riesgos en las fugas de información, utilizo una medición numérica y el

análisis de datos; Y en la cualitativa involucro la recolección de datos donde se utilizaron técnicas que no pretenden asociar las mediciones con números.

La forma que se procedió dentro de este enfoque integrador fue la siguiente:

- Primero se utilizaron técnicas cualitativas para comprender en su totalidad el fenómeno, y se logro una visión más amplia en los aspectos globales del mismo.
- A partir de esta primera incursión se refinaron las preguntas de investigación y se formuló la hipótesis.
- En la fase de recolección de datos para el análisis se utilizaron técnicas de ambos enfoques, unas que profundizaron en el conocimiento y otras lograron la precisión en los datos que permitieron asumir conclusiones y generalizaciones a partir.

Entre las técnicas que se utilizaron en este enfoque fueron: la observación no estructurada, entrevistas abiertas, revisión de documentos, discusión grupal y las historias de vida.

El diseño de este estudio fue de tipo **descriptiva** ya que dio a conocer las situaciones, costumbres y actitudes predominantes; A través de la descripción exacta de: las actividades, objetos, procesos y personas. No se limitó a la recolección de datos, sino a la predicción e identificación de las relaciones que existen entre dos o más variables de riesgo. Es también una investigación **no experimental** porque son datos que se tomaron de una norma la cual ya ha sido utilizada anteriormente.

Como principales fuentes de investigación que se tomaron son las secundarias, ya que se utilizaron: libros de texto, artículos de revistas, críticas literarias, comentarios, enciclopedias y biografías. Sin descartar las fuentes primarias como: documentos originales, apuntes de investigación, noticias y discursos de la empresa.

Entre los instrumentos que se utilizaron para la recolección de datos fueron: los cuestionarios, las escalas de actitudes y el análisis documental. Los cuales estuvieron compuestos por un conjunto

de preguntas con respecto a cada variable que estuvieron sujetas a medición, y que fueron elaborados tomando en cuenta los objetivos de la investigación.

La población de estudio se enfoco a la empresa E&B Promoción Empresarial S.A. de C.V. que se desarrolla en el ramo de promoción de marcas, aplicado desde altos puestos gerenciales, usuarios hasta el departamento de control interno que tenga acceso a la información.

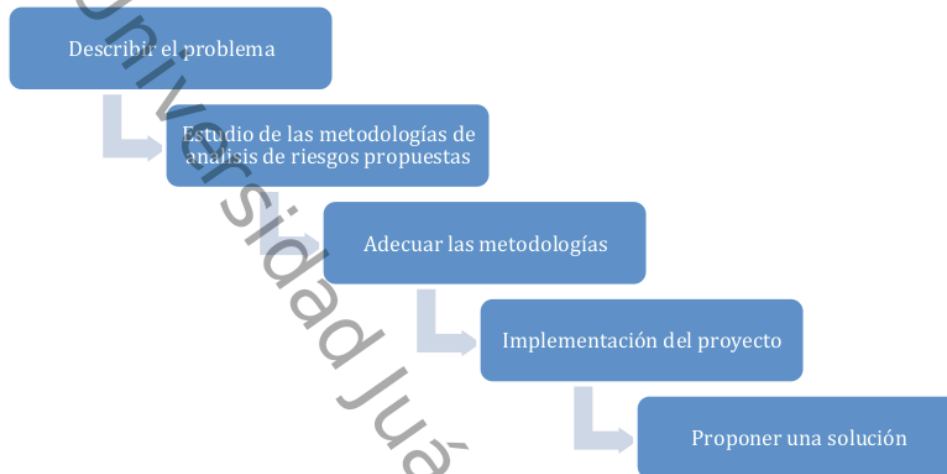
1.6.1 Metodología de la investigación

La forma de proceder dentro de este enfoque integrador es la siguiente:

1. Primero se utilizan técnicas cualitativas para comprender en su totalidad el fenómeno, logrando una visión más amplia en los aspectos globales del mismo.
2. A partir de esta primera incursión se refinan las preguntas de investigación y se formulan las problemáticas.
3. En la fase de recolección de datos para el análisis se utilizan técnicas de ambos enfoques, unas para profundizar en el conocimiento del mismo y otras para lograr precisión en los datos que permitan asumir conclusiones y generalizaciones a partir de estos.

Es por todo lo anterior que se propone la siguiente metodología para la realización de este proyecto:

Ilustración 1 Metodología a utilizar



Con el fin de realizar esta investigación se hará un análisis de las tres metodologías mencionadas en los antecedentes, tomando en cuenta el ciclo de contra-inteligencia para ver cuál es la que se adecue o las que se adecuen a E&B promoción empresarial y finalmente cubrir todas las áreas de oportunidad que se vayan presentando.

En la publicación de la metodología de análisis y gestión de riesgos de los sistemas de información en el libro 1 de método describe MAGERIT como una aproximación metódica para determinar el riesgo que sigue unos pasos pautados los cuales son: (Ministerio de administraciones publicas, 2006):

11

1. Determinar los activos relevantes para la organización, su interrelación y su valor, en el sentido de qué perjuicio (coste) supondría su degradación.
2. Determinar a qué amenazas están expuestos aquellos activos.
3. Determinar qué salvaguardas hay dispuestas y cuán eficaces son frente al riesgo.
4. Estimar el impacto, definido como el daño sobre el activo derivado de la materialización de la amenaza.
5. Estimar el riesgo, definido como el impacto ponderado con la tasa de ocurrencia (o

expectativa de materialización) de la amenaza.

Con el objeto de organizar la presentación, se tratan primero los pasos 1, 2, 4 y 5, obviando el paso 3, de forma que las estimaciones de impacto y riesgo sean “potenciales”: caso de que no hubiera salvaguarda alguna desplegada. Una vez obtenido este escenario teórico, se incorporan las salvaguardas del paso 3, derivando estimaciones realistas de impacto y riesgo.

MEHARI proporciona un enfoque estructurado para la evaluación del riesgo, basándose en unos simples principios. Una situación de riesgo se puede caracterizar por diferentes factores (MEHARI, 2010):

- Factores estructurales (u organizacionales), los cuales no dependen de medidas de seguridad, sino de la actividad principal de la organización, su entorno y su contexto.
- Factores de reducción del riesgo, que son una función directa de las medidas de seguridad implementadas.

El método MEHARI maneja en las evaluaciones de seguridad integra, cuestionarios de controles de seguridad, lo que permite evaluar el nivel de calidad de los mecanismos y soluciones encaminadas a la reducción del riesgo. Una fortaleza esencial de MEHARI es su capacidad de evaluar el nivel de riesgo actual así como el nivel futuro en base a una base de datos experta de conocimientos para evaluar el nivel de la calidad de las medidas de seguridad. Entre las evaluaciones que se realizan para elaborar este estudio están:

- Revisión de vulnerabilidades, un elemento del análisis de riesgos.
- Planes de seguridad basados en la revisión de vulnerabilidades.
- Apoyo de las bases de datos de conocimiento en la creación de un marco de referencia de seguridad.
- Construyendo el marco de referencia de seguridad.
- Gestionando las excepciones desde las reglas.
- Dominios cubiertos por el módulo de evaluación de vulnerabilidades.

- Descripción general del módulo de evaluación.

La seguridad en cualquier organización debe estar en consonancia con sus riesgos. Sin embargo, el proceso para determinar qué controles de seguridad son adecuados y rentables, es a menudo complejo y responde en gran medida a cuestiones subjetivas. Una de las principales funciones de análisis de riesgos de seguridad es poner este proceso en una base más objetiva (Pechuan, 1996).

Ahora bien con respecto a la Métrica versión 3 los procesos de su estructura principal son los siguientes (Públicas, 2009):

- Planificación de sistemas de información.
- Desarrollo de sistemas de información.
- Mantenimiento de sistemas de información.

El enfoque del proceso de planificación de sistemas de información, al no estar dentro del ámbito de la norma ISO 12.207 de procesos del ciclo de vida de software, se ha determinado a partir del estudio de los últimos avances en este campo, la alta competitividad y el cambio a que están sometidas las organizaciones. Métrica versión 3 ayuda en la planificación de sistemas de información facilitando una visión general necesaria para posibilitar dicha integración y un modelo de información global de la organización.

En cuanto al proceso de desarrollo de sistemas de información, para facilitar la comprensión y dada su amplitud y complejidad se ha subdividido en cinco procesos:

- Estudio de viabilidad del sistema (EVS).
- Análisis del sistema de información (ASI).
- Diseño del sistema de información (DSI).
- Construcción del sistema de información (CSI).
- Implantación y aceptación del sistema (IAS).

El proceso de mantenimiento de sistemas de información comprende actividades y tareas de modificación o retirada de todos los componentes de un sistema de información (hardware, software, operaciones manuales, redes, etc.). Este marco de actuación no es el objetivo de Métrica versión 3, ya que esta metodología está dirigida principalmente al proceso de desarrollo del software. Por lo tanto, refleja los aspectos del mantenimiento, correctivo y evolutivo, que tienen relación con el proceso de desarrollo.

Capítulo II. Marco Teórico

2.1 Marco conceptual

Dentro de este capítulo se muestra una visión amplia de los conceptos básicos relacionados con la seguridad de la información, así como también una serie de terminologías que se emplean en el desarrollo del estudio. Se muestran antecedentes y los actores sociales involucrados en el problema de la seguridad de información.

2.1.1 Inteligencia competitiva

Encierra un proceso sistemático de colecta, tratamiento, análisis y diseminación de la información; Sobre las actividades de los concurrentes, tecnologías y tendencias generales de los negocios, visando subsidiar la toma de decisión y alcanzar las metas estratégicas de la organización. En sentido amplio, el empleo de la inteligencia competitiva (IC en adelante) fuerza a las organizaciones a que mantengan un foco de rastreo externo continuo. Es más que estudiar los competidores; Es el proceso de estudiar cualquier cosa que pueda hacer la organización más competitiva y posicionarla mejor en el mercado (Unisul, 2005).

2.1.2 Contrainteligencia empresarial

Conocida como ⁹ inteligencia empresarial defensiva, se refiere al uso de los datos de una empresa para facilitar la toma de decisiones a las personas que deciden, es decir, la comprensión del funcionamiento actual y la anticipación de acciones para dar una dirección bien informada a la empresa. Las herramientas de inteligencia se basan en la utilización de un sistema de información de inteligencia que se forma con distintos datos extraídos de los datos de producción, con información relacionada con la empresa o sus ámbitos y con datos económicos (Ettore, 1995).

También es conocida como todas aquellas medidas de carácter pasivo o activo que realiza una empresa pública o privada para evitar las acciones de Inteligencia Empresarial o del adversario en contra de ellas. (Gómez, 2002)

Según una revista hispana son aquellas actividades orientadas a proteger la propiedad intelectual en la que se sustenta la estabilidad competitiva de una organización y la prevención de acciones hostiles por partes de posibles contendientes (Comai, 2003).

28 La siguiente figura muestra el ciclo de producción de contra-inteligencia empresarial (CCI), que consiste en un modelo conceptual para la protección de ventajas competitivas conquistadas. Didácticamente, aunque eso sea una abstracción, el ciclo caracteriza fases distinguidas del proceso de evitar en los rivales los insights de valor y la protección de las informaciones sensibles (Miller, 2002).



Ilustración 2 Ciclo contrainteligencia

2.1.3 Activos

En el diccionario (fistierra, 2011), un activo es todo aquel bien o derecho que posee una persona física o jurídica que puede convertirse en liquidez, es decir, que se puede valorar en términos monetarios.

En el plan general de contabilidad español se definen los activos como bienes, derechos y otros recursos controlados económicamente por la empresa, resultantes de sucesos pasados de los que se espera obtener beneficios o rendimientos económicos en el futuro (Plan General Contable, 2007).

2.1.4 Dato

(Tecnología, 2008) Precisa que proviene del latín datum (“lo que se da”), un dato es un documento, una información o un testimonio que permite llegar al conocimiento de algo o deducir las consecuencias legítimas de un hecho.

La definición que nos brinda (D'Ambrosio, 2009) el dato es una representación simbólica (numérica, alfabética, algorítmica etc.), un atributo o una característica de una entidad. El dato no tiene valor semántico o sentido en sí mismo, pero si recibe un tratamiento apropiado, se puede utilizar en la realización de cálculos o toma de decisiones entonces entendemos que los datos son comunicados por varios tipos de símbolos tales como las letras del alfabeto, números, movimientos de labios, puntos y rayas, señales con la mano, dibujos, etc. Estos símbolos se pueden ordenar y reordenar de forma utilizable y se les denomina información.

De lo anterior se concreta que los datos son símbolos que describen condiciones, hechos, situaciones o valores. Y se caracterizan por no contener ninguna información. Un dato puede significar un número, una letra, un signo ortográfico o cualquier símbolo que represente una cantidad, una medida, una palabra o una descripción.

En el libro “La revolución de la riqueza”, nos brindan la siguiente diferencia entre lo que son los datos y lo que es información: “Los datos suelen ser descritos como elementos discretos, huérfanos de contexto: por ejemplo, 300 acciones. Cuando los datos son contextualizados, se convierten en información: por ejemplo, tenemos 300 acciones de la empresa farmacéutica X” (Toffler & Toffler, 2006).

2.1.5 Conocimiento

26 No existe una definición de “Conocimiento”. Sin embargo existen muchas perspectivas desde las que se puede considerar el conocimiento, siendo un problema histórico de la reflexión filosófica y de la ciencia la consideración de su función y fundamento.

Para el filósofo griego en el diccionario electrónico Platón, el conocimiento es aquello necesariamente verdadero (episteme). En cambio, la creencia y la opinión ignoran la realidad de las cosas, por lo que forman parte del ámbito de lo probable y de lo aparente. Nos precisa en definición más concreta que es conjunto de información almacenada mediante la experiencia o el aprendizaje (a posteriori), o a través de la introspección (a priori). En el sentido más amplio del término, se trata de la posesión de múltiples datos interrelacionados que, al ser tomados por sí solos, poseen un menor valor cualitativo (Definición, 2008).

2.1.6 Información

21 Cada vez que deseamos conocer algo acerca de acontecimientos, hechos, sucesos, personas, empresas, instituciones ciudades, países, etc. ya sea porque necesitamos reducir nuestra incertidumbre para tomar decisiones o simplemente porque queremos incrementar nuestro conocimiento acerca de algo, buscamos aquello que denominamos «información». Y esto, es algo que hacemos, en mayor o menor medida, todos los días.

23 Para entender más este término Chiavetano nos dio a conocer su significado como “un conjunto de datos con un significado, o sea, que reduce la incertidumbre o que aumenta el conocimiento de

algo. En verdad, la información es un mensaje con significado en un determinado contexto, disponible para uso inmediato y que proporciona orientación a las acciones por el hecho de reducir el margen de incertidumbre con respecto a nuestras decisiones" (Idalberto, 2006).

En relación a todas estas definiciones conceptuales encontré una descrita por (Thompson, 2008) en una web que la sitúa como "Un conjunto de datos acerca de algún suceso, hecho o fenómeno, que organizados en un contexto determinado tienen su significado, cuyo propósito puede ser el de reducir la incertidumbre o incrementar el conocimiento acerca de algo".

Damos por información a una parte de suma importancia para alguna persona o empresa dependiendo el caso en el que sea utilizada. En una sociedad la conducta de cada individuo frente a algunos otros individuos se puede ver alterada en función de qué información disponible posee el primer individuo.

2.1.6.1 Tipos de información

Como se ha descrito la información en la actualidad es un activo importante con respecto a una empresa o persona que la utilice ya que contendrá datos valiosos. El tipo de información creada depende de las relaciones definidas entre los datos existentes, adicionar datos nuevos o diferentes significa la posibilidad de redefinir las relaciones.

Para esto (Soto, Mi tecnologico, 2009) en su sitio web nos presenta a la información en 3 tipos y las clasifica según su relevancia:

- Información pública: Es la que cualquier persona puede acceder. Este tipo de información es vital para conseguir logros comerciales, pero es un error dirigirla únicamente al exterior de la empresa. Todos los integrantes de una empresa o de un proyecto deben estar al corriente sobre la información que cualquier usuario puede obtener.
- Información interna: Todos los datos y contenidos necesarios para llevar a cabo un proyecto, así como las informaciones relativas a la propia empresa que se ponen en

conocimiento de todo el equipo. Esta es en relación a información perteneciente a un determinado grupo selecto de personas que se encuentran dentro de una empresa sin ningún interés por compartirla a personas ajenas a ella.

- Información privada: la que no puede ir más allá de las personas que deban manejarla. Datos concretos sobre la contabilidad, nuevas ideas en fase de definición, negociaciones en marcha, datos internos de clientes, filtraciones y rumores que no se propaguen, etc. Claro está que la persona que maneja esta información tiene mayor grado de responsabilidad ya que tienen un alto grado de confianza.

2.1.6.2 Amenazas a la información

En cuanto a los tipos de riesgos que se implican en los sistemas de información, según publica el CERT® Coordination Center, la mayoría de las amenazas recibidas cuando se está conectado constituyen casos de cibercrimen (CCN- Cert Seguridad TiC, 2007), la situación actual se caracteriza por:

- Los tipos de amenazas evolucionan continuamente (virus, phishing, defacement, etc.).
- Los sistemas de información para misiones críticas de las organizaciones se están integrando cada vez más con Internet.
- El daño y la velocidad de los ataques se incrementan continuamente.
- El software continúa teniendo vulnerabilidades intrínsecas "desde la caja".
- Existe un amplio consenso en considerar que el cibercrimen es una debilidad crítica de las naciones occidentales.

2.1.6.3 Tipos de amenazas

Existen diferentes tipos de amenazas que pueden clasificar entre las que son provocadas y las que se generan por descuido. Entre las amenazas informáticas más comunes según son los (Panda Security, 2011):

- Virus
- Gusanos
- Troyanos
- Adware
- Spyware
- Rootkits
- Exploits
- Dialers
- Cookies
- Phishing
- Spam
- Redes de boots
- Scams

Conviene distinguir que estas amenazas ocupan un espacio en el lenguaje cotidiano ya que son utilizadas en la seguridad mas básica de un computador en un hogar, sin necesidad de ser expertos en el tema.

De lo anterior se puede afirmar las amenazas son cada vez mas constantes y que pueden ocurrir en cualquier momento, a continuación se mencionan algunos tipos de amenazas mostrados en el blog de seguridad de la información (ingwebsu, 2008):

- Físicas: los puntos débiles de orden físico son aquellos presentes en los ambientes en los cuales la información se está manejando o almacenando físicamente. Ejemplos: Instalaciones inadecuadas del espacio de trabajo y ausencia de recursos para el combate a incendios.
- Naturales: son aquellos relacionados con las condiciones de la naturaleza que puedan colocar en riesgo la información ejemplos: Ambientes sin protección contra incendios, locales próximos a ríos propensos a inundaciones e infraestructuras incapaces de resistir a las manifestaciones de la naturaleza como terremotos, maremotos, huracanes etc.
- De hardware: los posibles defectos en la fabricación o configuración de los equipos de la empresa que pudieran permitir el ataque o alteración de los mismos. Ejemplos: La ausencia de actualizaciones conforme con las orientaciones de los fabricantes de los programas que se utilizan y Conservación inadecuada de los equipos.
- De software: los puntos débiles de aplicaciones permiten que ocurran accesos indebidos a sistemas informáticos incluso sin el conocimiento de un usuario o administrador de red. Ejemplos: Programas lectores de e-mail que permiten la ejecución de códigos maliciosos, editores de texto que permiten la ejecución de virus de macro etc. y programas para la

automatización de procesos.

- De almacenamiento: como son el plazo de validez o caducidad y los defectos de fabricación.
- Humanas: intervienen lo que son las contraseñas débiles y el compartir identificadores tales como nombre de usuario o credencial de acceso.
- Contaminación: polvos, químicos y residuos.
- Integridad: autorización, restricciones, exactitud de entrada.
- Relación: uso no oportuno de la información, datos incorrectos o información de una persona/proceso/sistema en tiempo estimado
- Acceso: al inapropiado acceso a sistemas/datos/información y la confidencialidad de la información.
- Infraestructura: es la estructura de la información tecnológica efectiva ya sea hardware, software, redes personal y procesos; también interviene todo lo relacionado con el mantenimiento en los procesos de TI en desarrollo y que los equipos estén actualizados.
- Utilidad: técnicas de recuperación o restauración, backups y planes de contingencia.

2.1.7 Insiders

El diccionario económico financiero dice que es un ²⁹anglicismo con el que se designa a la persona que goza de información confidencial por razón de su cargo. El uso de esta información es en beneficio propio, de los allegados o de terceros que resulta ilegal (Diccionario economico financiero, 2009).

La enciclopedia británica nos dice que es la persona reconocida o aceptada como miembro de un grupo con categoría en una organización, que tenga acceso a información confidencial, que se encuentre en una posición de tener conocimientos comprometedores de la empresa (Merriam-Webster, 2012).

2.1.8 Seguridad de la información

La gerente de tecnología de información de consultora Grant Thorton, María Acevedo le da el significado de tomar las medidas preventivas o correctivas que logren resguardar y proteger la información de nuestra empresa (Acevedo, 2012).

En el portal del project management en español, refiere a la seguridad de la información como la confidencialidad, integridad, disponibilidad de la información y datos, independientemente en la forma en que los datos puedan estar: electrónicos, impresos u audio (Spanishpmo, 2009). En otras palabras, la seguridad de la información tiene como fin la protección de la información y de los sistemas de la información del acceso, uso, divulgación, interrupción o destrucción no autorizada.

2.1.8.1 Alcance de la seguridad informática

El alcance de la seguridad informática lo define cada organización, se comprende de acuerdo a la información que posee y el nivel de protección que se requiera. De acuerdo a la empresa de antivirus Panda security para que la seguridad informática cumpla con el alcance que tiene y cubra todos los rubros a proteger debe tener las siguientes características: (Panda Security, 2009).

- Políticas, normas, procedimientos y estándares de seguridad informática.
- Administración de usuarios y recursos de los diferentes sistemas informáticos o de comunicación.
- Seguridad interna de acceso a las aplicaciones.
- Normas y procedimientos de operaciones del centro de cómputos.
- Metodología de desarrollo, mantenimiento y control de cambios.
- Procedimiento de backup y recovery.
- Definición, desarrollo y mantenimiento de un plan de contingencias.
- Seguridad física de accesos, contra incendio, problemas eléctricos de centro de cómputos y lugar de resguardo de la información.

2.1.8.2 Seguridad lógica

El licenciado en economía Lauro Soto, define a la seguridad lógica como la que se encarga de los controles de acceso que están diseñados para salvaguardar la integridad de la información almacenada en una computadora, así como de controlar el mal uso de la información. Identifica individualmente a cada usuario, sus actividades en el sistema, restricción en el acceso a datos, a los programas de uso general, de uso específico, de las redes y los terminales. (Soto, Mi Tecnológico, 2008).

Cristian F. Borghello licenciado en Sistemas de seguridad de información define la seguridad lógica como la aplicación de barreras y procedimientos que resguarden el acceso a los datos que sólo se permita acceder a ellos a las personas autorizadas para hacerlo. Existe un viejo dicho en la seguridad informática que dicta que “todo lo que no está permitido debe estar prohibido” y esto es lo que debe asegurar la Seguridad Lógica (Borghello C. , 2009).

Por lo tanto, se concluye que la seguridad lógica es la correcta aplicación de controles para resguardar el acceso a la información de la empresa, con el objeto de minimizar el riesgo de hacer un mal uso de ésta, asegurando su integridad y, conjuntamente, procurar que solo sea manejada por el personal apropiado.

1 **Controles de acceso lógico:** Mireya Delgado en el manual de preparación CISA menciona que el concepto de control de acceso se refiere a administrar y controlar el acceso a los recursos de información de una organización que reside en sistemas de computadora basados en anfitriones y en la red. Los controles inadecuados de acceso lógico aumentan el potencial de una organización de pérdidas resultantes de las exposiciones (Debali, Manual de Preparación al Examen CISA, 2008). Estas exposiciones pueden tener como consecuencia pequeños inconvenientes hasta un cierre total de las funciones de computación. Entonces, los controles de acceso lógico son el medio para administrar y proteger la información, para reducir riesgos a un nivel aceptable para una organización.

2.1.8.3 Seguridad física

El profesor Sergio Talens-Oliag de la Universidad de Valencia define la seguridad física como todos aquellos mecanismos de prevención y detección, destinados a proteger físicamente cualquier recurso del sistema; estos recursos son desde un simple teclado hasta una cinta de backup con toda la información que hay en el sistema, pasando por la propia CPU de la máquina. Dependiendo del entorno y los sistemas a proteger esta seguridad será más o menos importante y restrictiva, aunque siempre deberemos tenerla en cuenta (Talens-Oliag, 2009).

1 **Controles de acceso físico:** para evitar todo tipo de problemas en la pérdida de información se pueden implementar mecanismos de prevención (control de acceso a los recursos) y de detección es decir si un mecanismo de prevención falla o no existe, se debe al menos detectar los accesos no autorizados cuanto antes. Los controles de acceso físico están diseñados para proteger la organización contra los accesos no autorizados.

A continuación se mencionan algunos de los problemas de seguridad física en los cuales en un momento se puede enfrentar el usuario y las medidas a tomar en cuenta para evitarlos o al menos minimizar su impacto por Mireya Delgado, de los controles de acceso más comunes tenemos (Debali, Manual de Preparación al Examen CISA, 2008):

- 1** • Cerraduras con cerrojo: estas cerraduras requieren la llave tradicional de metal para lograr entrar.
- Cerraduras electrónicas: este sistema usa una llave o tarjeta magnética basada en chips integrados que se pasa por un lector sensor para entrar.
- Cerraduras biométricas: las características físicas únicas de una persona, como por ejemplo la voz, la retina, las huellas digitales o la firma, activan estas cerraduras.
- Cámaras de video: las cámaras deben estar ubicadas en puntos estratégicos y deben ser monitoreadas por guardias de seguridad. Las cámaras sofisticadas de video pueden ser activadas por movimiento.
- Sistema de alarma: un sistema de alarma debe estar conectado a los puntos de entrada

inactivos, a los detectores de movimientos y al flujo inverso de ingreso para las puertas que son exclusivamente de salida.

2.1.9 Delito informático

El portal de informática, internet y tecnologías Alegsa dice que el delito informático implica cualquier actividad ilegal que encuadra en figuras tradicionales ya conocidas como robo, hurto, fraude, falsificación, perjuicio, estafa y sabotaje, pero siempre que involucre la informática de por medio para cometer la ilegalidad (Alegsa, 2009).

El constante progreso tecnológico que experimenta la sociedad, supone una evolución en las formas de delinquir, dando lugar, tanto a la diversificación de los delitos tradicionales como a la aparición de nuevos actos ilícitos. Esta realidad ha originado un debate en torno a la necesidad de distinguir o no los delitos informáticos del resto.

Diversos autores y organismos han propuesto definiciones de los delitos informáticos, aportando distintas perspectivas y matices al concepto. Algunos consideran que es innecesario diferenciar los delitos informáticos de los tradicionales, ya que, según éstos se trata de los mismos delitos, cometidos a través de otros medios.

¹⁹ La Organización de las Naciones Unidas define tres tipos de delitos informáticos (ONU, 2005):

- Fraudes cometidos mediante manipulación de computadoras.
- Manipulación de los datos de entrada.
- Daños o modificaciones de programas o datos computarizados.

Los fraudes cometidos mediante manipulación de computadoras pueden clasificarse en:

- Manipulación de los datos de entrada o sustracción de datos.

- La manipulación de programas: modificación de programas existentes en un sistema o la inserción de nuevos programas.
- Manipulación de los datos de salida.

Los fraudes cometidos mediante la manipulación de los datos de entrada:

- Como objeto: alteración de los documentos digitales.
- Como instrumento: uso de las computadoras para falsificar documentos de uso comercial.

Los daños o modificaciones de programas o datos computarizados:

- Sabotaje informático: acción de eliminar o modificar funciones o datos en una computadora sin autorización, para obstaculizar su correcto funcionamiento.
- Acceso no autorizado a servicios y sistemas informáticos.
- Reproducción no autorizada de programas informáticos de protección legal: ver piratería.

2.1.10 Ataques informáticos

Los ataques pueden ser del tipo pasivos o activos, y el personal realiza ambos indistintamente dependiendo de la situación concreta a como los describe Cristian Borghello en su página web pueden ser: personales interno, ex-empleados, curiosos, terroristas o intrusos remunerados (Borghello C. F., 2009).

2.1.10.1 ² Personal interno

Las amenazas a la seguridad de un sistema, provenientes del personal del propio sistema informático, rara vez es tomada en cuenta porque se supone un ámbito de confianza. Generalmente estos ataques son accidentes por desconocimiento o inexistencia de las normas básicas de seguridad; pero también pueden ser del tipo intencional.

2.1.10.2 Ex-empleado

Este grupo puede estar especialmente interesado en violar la seguridad de la empresa, sobre todo aquellos que han sido despedidos y no han quedado conformes; o bien aquellos que han renunciado para pasar a trabajar en la competencia. Generalmente se trata de personas descontentas con la organización que conocen a la perfección la estructura del sistema y tienen los conocimientos necesarios como para causar cualquier tipo de daño. También han existido casos donde el ex-empleado deja bombas lógicas que "explotan" tiempo después de marcharse.

2.1.10.3 Curiosos

Suelen ser los atacantes más habituales del sistema. Son personas que tienen un alto interés en las nuevas tecnologías, pero aún no tienen los conocimientos ni experiencia básicos para considerarlos hackers o crackers (podrían ser Newbies). En la mayoría de los casos son estudiantes intentando penetrar los servidores de su facultad o empleados consiguiendo privilegios para obtener información para él vedada. Generalmente no se trata de ataques de daño pero afectan el entorno de fiabilidad con confiabilidad generado en un sistema.

2.1.10.4 Terroristas

² Bajo esta definición se engloba a cualquier persona que ataca el sistema para causar daño de cualquier índole en él; y no sólo a la persona que coloca bombas o quema automóviles. Son ejemplos concretos de este tipo, ataque de modificación de los datos de clientes entre empresa competidoras, o de servidores que albergan páginas web, bases de datos entre partidos políticos contrarios, etc.

2.1.10.5 Intrusos Remunerados

² Este es, sin duda, el grupo de atacantes más peligroso, aunque también el menos habitual. Se trata de crackers o piratas con grandes conocimientos y experiencia, pagados por una tercera parte para

robar "secretos" (código fuente de programas, bases de datos de clientes, información confidencial de satélites, diseño de un nuevo producto, etc.) o simplemente para dañar, de alguna manera la imagen de la entidad atacada. Suele darse, sólo, en grandes multinacionales donde la competencia puede darse el lujo de un gran gasto para realizar este tipo de contratos y contar con los medios necesarios para realizar el ataque.

2.1.11 Políticas de seguridad

Según el manual de preparación al examen CISA ¹ las políticas son documentos de alto nivel que representan la filosofía corporativa de una organización y el pensamiento estratégico de la alta gerencia y de los dueños del proceso de negocio (Debali, Manual de preparación al examen CISA, 2008). Las políticas deben ser claras y concisas para que sean efectivas. La administración debe crear un ambiente positivo de control asumiendo la responsabilidad de formular, desarrollar, documentar, promulgar y controlar las políticas que abarcan las metas y las directrices generales.

2.1.11.1 Controles de seguridad de la información:

Los controles se pueden clasificar en tres principales categorías: administrativos, físicos y técnicos.

Controles Físicos: ⁸ limitan el acceso físico directo a los equipos. Consisten en cerraduras, bloqueos para teclados, vigilantes de seguridad, alarmas y sistemas ambientales para la detección de agua, fuego y humo. Los controles físicos también incluyen a los sistemas de respaldo, alimentación de reserva (UPS), documentación de reserva, detectores de movimiento, rendijas, detectores de humo, guardias de seguridad, monitorización de circuito cerrado, tarjetas de identificación, sensores, alarmas, controles biométricos de acceso y extintores contra incendios.

Controles Administrativos: ⁷ incluyen las políticas y procedimientos de seguridad. Las políticas establecen lo que los usuarios pueden y no pueden hacer al utilizar los recursos informáticos de la organización. También incluyen procedimientos para la renovación de claves de acceso,

autorizaciones para acceder a sus recursos, la revisión, validación periódica de la vigencia del tipo de acceso, la asignación de responsabilidades, conocimientos de la seguridad, formación técnica, gestión, supervisión de las tecnologías, soluciones aplicadas, la recuperación tras averías o fallos, la realización y la aplicación de planes de contingencia.

Los controles administrativos también incluyen la revisión de seguridad e informes de auditoría, que se utilizan para identificar si los usuarios siguen las políticas y procedimientos. Cada persona de la organización debe tener claras sus responsabilidades relativas a la seguridad de cada componente a su cuidado, estas responsabilidades se deben incluir en los objetivos de cada persona para asegurar que se les valore según la responsabilidad asignada y se les evalúe por su cumplimiento de obligaciones.

Entre los controles administrativos podemos destacar:

- Conocimientos de seguridad, formación técnica revisiones y auditorías de seguridad.
- Separación de obligaciones control de calidad.
- Procedimientos sancionadores e investigaciones de antecedentes.
- Políticas, procedimientos de seguridad y rotación de responsabilidades.
- Gestión y supervisión.
- Recuperación de fallos y planes de contingencia.
- Administración de accesos de usuarios.
- Gestión de propietarios de datos y recursos.

Controles Técnicos: implantan a través de soportes físicos o lógicos que típicamente son difíciles de vencer, una vez implantados, pueden funcionar sin la intervención humana. El soporte lógico específico incluye antivirus, firmas digitales, cifrado, programas de control de biblioteca, herramientas de gestión de red, contraseñas, tarjetas inteligentes, control de acceso de llamadas, sistemas de re-llamada, seguimiento de huellas y sistemas expertos de detección de intrusiones.

8

El no-repudio previene la posibilidad de que una de las partes de un intercambio o transacción niegue en falso después que haya tenido lugar la misma. El control técnico que se emplea para garantizar el no-repudio es la firma digital. Las operaciones comerciales celebradas a través de redes internas e internet se han vuelto corrientes. Allí donde antes se empleaba una firma manuscrita para verificar que se había hecho una compra o celebrado un determinado contrato, ahora existe una alternativa digital para verificar que una persona cumplirá con sus obligaciones.

7

La firma digital consiste en una clave privada que sólo conoce o puede duplicar el dueño de la clave, parecida a su firma y rúbrica manuscrita. Las firmas digitales verifican la fuente, autenticidad e integridad de mensajes electrónicos. Ejemplos:

- Programas de control de acceso, log's y bitácoras para auditoría.
- Programas cortafuegos, antivirus y sistemas expertos de detección de intrusiones.
- Gestión de contraseñas.
- Controles técnicos.

Los tres controles de seguridad que se mencionan también se pueden subdividir en:

- Preventivos: intentan evitar la ocurrencia de acontecimientos indeseados.
- Correctivos: intentan identificar los incidentes y reducir sus efectos después de que hayan sucedido, identificar el problema con suficiente rapidez para reducir los daños al mínimo y para poder valorar con precisión la magnitud de los daños causados por el incidente.

2.1.12 Amenazas

El instituto nacional de las tecnologías de la comunicaciones clasifica a las distintas amenazas en que la información puede ser sometida, en tres rubros principales que son (INTECO-CERT, 2009):

8

- Las amenazas intencionadas: las ejercen usuarios no autorizados que acceden de forma

indebida a los datos o información sensible. Los usuarios no autorizados pueden ser externos o pertenecientes a la propia organización y se pueden clasificar como curiosos o maliciosos.

- Las amenazas no intencionadas: provienen típicamente de empleados con poca formación o negligentes que no han seguido los pasos para proteger sus contraseñas, asegurar adecuadamente sus ordenadores o actualizar con la frecuencia debida el programa antivirus.
- Las amenazas naturales: incluyen fallos de equipos y calamidades tales como incendios, inundaciones y terremotos que pueden causar la pérdida de equipos y datos. Las amenazas naturales suelen afectar a la disponibilidad de los recursos y de la información.

2.1.13 Riesgos

Los riesgos existen en cada nivel de las organizaciones. Cada sistema está constituido por una serie de procesos, a su vez formados por actividades manuales o automatizadas que podrían estar relacionadas a un error o riesgo potencial.

Según Leonor Galán Quiroz el riesgo se define como una situación con dos características: Probabilidad de ocurrencia y Efecto negativo que no deseamos, directamente relacionado con la pérdida financiera (Galán Quiroz, 1996).

Ante un riesgo concreto la organización tiene tres alternativas: aceptar el riesgo, hacer algo para disminuir la posibilidad de ocurrencia del riesgo o transferir el riesgo.

2.1.13.1 Tipos de riesgos

Con las definiciones anteriores podemos destacar que existen un sin número de tipos de riesgos en los que se puede ver afectado los activos de la información, según el artículo publicado sobre riesgos de la información por la Alianza Empresarial para el Comercio Seguro de Costa Rica

(BASC por sus siglas en ingles) los riesgos comúnmente se presentan y serán tomados para el análisis son: (Business Alliance for Secure Commerce, 2010):

- Robo o extravío: consistente en el apoderamiento de bienes ajenos en este caso la información, con intención de lucrarse o por otra parte perdida de información con fin de lucro.
- Ambientales: abarcan lo que son problemas climáticos o circunstanciales en este caso pueden ser: inundaciones, incendios, huracanes, sismos y las lluvias.
- Contaminación: se toma en cuenta los factores como son: polvo, humeado, químicos y los residuos (basura).
- Integridad: riesgo que involucra al personal con uso de información sin autorización y las restricciones es decir, administración inadecuada de controles, bajo o nulo mantenimiento en el área de sistemas.
- Relación: se refiere al uso no oportuno de la información. Se resume a la relación que existe entre los sistemas de información/ datos/ personas/ procesos/ sistemas correctos.
- Accesos: se entiende por la confidencialidad que se tiene y al inapropiado acceso a sistemas, datos e información.
- Infraestructura: llámese al conjunto de herramientas actualizadas y seguras en el uso de la información (hardware, software, redes y procesos).
- Utilidad: estos riesgos se enfocan a las técnicas de recuperación (backups, puntos de restauración) o planes de contingencia.
- Seguridad general: aquí intervienen riesgos por descargas eléctricas, incendios, radiaciones, fallas mecánicas etc.

2.1.14 Impacto

18

La proliferación de los delitos informáticos ha hecho que nuestra sociedad sea cada vez más escéptica a la utilización de tecnologías de la información, las cuales pueden ser de mucho beneficio para la sociedad en general. Este hecho puede obstaculizar el desarrollo de nuevas formas de hacer negocios, por ejemplo el comercio electrónico puede verse afectado por la falta

de apoyo de la sociedad en general (Campos, 2004).

Algunas de las empresas que poseen activos informáticos importantes, son cada vez más celosas y exigentes en la contratación de personal, pudiendo afectar en forma positiva o negativa a la sociedad laboral de nuestros tiempos. La falta de cultura informática puede impedir de parte de la sociedad la lucha contra los delitos informáticos, por lo que el componente educacional es un factor clave en la minimización de esta problemática.

2.1.15 DLP

Uno de los líderes a nivel mundial de seguridad de contenidos de internet y cloud computin describe a la pérdida de datos o DLP por sus siglas en ingles (Data Loss Prevention) que es un elemento básico para detener las filtraciones de datos accidentales y malintencionadas, pueda tratarse de información de clientes, datos financieros, propiedad intelectual o secretos comerciales. Un incidente puede costar millones de dólares por deterioro de la imagen de marca, oportunidades de negocio perdidas, multas y procesos judiciales (Trendmicro, 2010).

Otra empresa reconocida también por brindar seguridad a la información describe DLP como una solución efectiva para evitar fugas de información orientada hacia empresas de tamaño mediano o grande, que manejan datos sensibles y no se pueden permitir fugas de información también nos permite localizar dónde se encuentra la información sensible almacenada, crear un inventario de los datos, supervisar de qué forma se utilizan estos datos y si alguien está infringiendo la política corporativa de protección de datos para evitar que estos salgan de la organización. Nos permite crear políticas para gestionar todas estas tareas de protección de nuestros datos (Symantec, 2009).

2.1.16 Método MAGERIT

El método de MAGERIT descrita en la publicación (Ministerio de administraciones publicas, 2006) elaborado por el Consejo Superior de Administración Electrónica (CSAE) publica su primer versión en 1997, nos define; que es un método formal para investigar los riesgos que

soportan los Sistemas de información, se encarga de recomendar las medidas apropiadas que deberían adoptarse para controlar estos riesgos, a su vez es un instrumento para facilitar la implantación y aplicación del esquema nacional de seguridad, proporcionando los principios básicos y requisitos mínimos para la protección adecuada de la información.

2.1.17 Análisis de riesgos

El análisis de riesgos es una aproximación metódica para determinar el riesgo. La consultora de seguridad de la información describe al análisis de riesgo como ³³ piedra angular de la que se apoyan las acciones en la selección de controles y aplicar, e incluso la base para elaborar planes directores o parciales de seguridad o un plan de continuidad del negocio (ESA-security, 2009).

El ministerio de administraciones publicas de España precisa un riesgo como un evento, el cual es incierto y tiene un impacto negativo en el análisis de riesgo como en el proceso cuantitativo o cualitativo que permite evaluar los riesgos. El proceso de análisis de riesgos, se basa en (Ministerio de administraciones publicas, 2006):

1. Creación de un inventario de activos.
2. Simplificación de activos en dominios.
3. Detección de vulnerabilidades y amenazas asociadas. Se utilizan como complemento los servicios de hacking ético si así se solicita.
4. Evaluación de probabilidades e impactos.
5. Análisis de controles ISO implantados.
6. Obtención del riesgo.

2.1.17.1 Enfoques para el análisis de riesgos

Existen una serie de diferentes enfoques para el análisis de riesgos pero, en esencia, suelen dividirse en dos tipos fundamentales: cuantitativos y cualitativos como lo describe la directora de

consultoría Beatriz Martínez para la empresa dedicada a la protección de sistemas de la información que habla de los riesgos en la informática (Martínez, 2007):

- **Enfoque cuantitativo:**

Este enfoque emplea dos elementos fundamentales, la probabilidad de que se produzca un hecho y la probable pérdida en caso de que ocurra el hecho citado. El enfoque cuantitativo de análisis de riesgos se centra en el uso de una sola cifra producida a partir de estos elementos. A esto se le suele denominar comúnmente el “Annual Loss Expectancy” – ALE (Esperanza de pérdida anual) o también “Estimated Annual Cost” – EAC (Coste anual estimado). La forma de calcularlo para un evento en concreto se realiza mediante la multiplicación de la pérdida potencial por la probabilidad. Gracias a este enfoque, es teóricamente posible clasificar los acontecimientos en orden de riesgo a fin de tomar decisiones sobre esta base.

Los problemas con este tipo de análisis de riesgos están generalmente asociados con la inexactitud y falta de fiabilidad de los datos. Los datos asociados a las probabilidades (estimadas por lo general bajo el criterio interno de la empresa) rara vez suelen ser precisos y pueden, en algunos casos, estar basados en la propia autocomplacencia de los dueños de los procesos de negocio. Además, los controles y las contramedidas a menudo hacen frente a una serie de posibles acontecimientos en los que los hechos que los producen están normalmente interrelacionados. A pesar de estos inconvenientes, son numerosas las organizaciones que han adoptado y aplicado con éxito el análisis de riesgos cuantitativos.

- **Enfoque cualitativo:**

Es la metodología más utilizada para el análisis de riesgos. En este caso, la probabilidad no es necesaria y tan solo es utilizado como factor de cálculo la pérdida potencial estimada. Para compensar esta situación, la mayoría de las metodologías de análisis de riesgo cualitativo hacen uso de una serie de elementos relacionados entre sí.

2.1.18 MEHARI

Una contribución importante del CLUSIF a la gestión de los riesgos relacionados con la información es proporcionada por la evaluación de riesgos de información y gestión método MEHARI, en torno a un amplio conjunto de módulos, herramientas y cuestionarios.

MEHARI se distribuye bajo los principios de código abierto, responde a la norma ISO / IEC 27005:2008 directrices para la gestión de riesgos y permite mayor control de la conformidad de las organizaciones de un proceso de SGSI ISO 27001. Incluye, directamente en las bases de conocimiento, las fórmulas del método para la evaluación directa de los riesgos y la valoración de las formas de tratar y reducir los mismos, con base de conocimientos y la documentación proporcionada por CLUSIF en francés y en inglés, traducciones a otros idiomas también están disponibles gracias a las contribuciones voluntarias (MEHARI, 2010).

2.1.19 Métrica V3

Esta metodología ofrece a las organizaciones un instrumento útil para la sistematización de las actividades que dan soporte al ciclo de vida del software. Contempla el desarrollo de sistemas de información para las distintas tecnologías que actualmente están conviviendo y los aspectos de gestión que asegurarán que un proyecto cumpla sus objetivos en términos de calidad y costos.

En la elaboración de métrica versión 3 se han tenido en cuenta los métodos de desarrollo más extendidos, así como los últimos estándares de ingeniería del software y calidad, así como referencias específicas en cuanto a seguridad y gestión de proyectos.

2.1.20 Valores porcentuales

En matemáticas, un porcentaje es una forma de expresar un número como una fracción de 100 (por ciento, que significa “de cada 100”). Es a menudo denotado utilizando el signo porcentaje %, que se debe escribir inmediatamente después del número al que se refiere, sin dejar espacio de

separación.¹ Por ejemplo: "treinta y dos por ciento" se representa mediante 32% y significa 'treinta y dos de cada cien'. También puede ser representado como $32 / 100$.

2.1.20.1 Regla de tres

La regla de tres o regla de tres simple es una forma de resolver problemas de proporcionalidad entre tres o más valores conocidos y una incógnita. En ella se establece una relación de linealidad (proporcionalidad) entre los valores involucrados.

La regla de tres más conocida es la regla de tres simple directa, si bien resulta muy práctico conocer la regla de tres simple inversa y la regla de tres compuesta, pues son de sencillo manejo y pueden utilizarse para la resolución de problemas cotidianos de manera efectiva.

Regla de tres simple.

En la regla de tres simple, se establece la relación de proporcionalidad entre dos valores conocidos A y B, y conociendo un tercer valor X, calculamos un cuarto valor Y.

$$\begin{array}{lcl} A & \longrightarrow & B \\ X & \longrightarrow & Y \end{array}$$

La relación de proporcionalidad puede ser directa o inversa, será directa cuando a un mayor valor de A habrá un mayor valor de B, y será inversa, cuando, a un mayor valor de A corresponda un menor valor de B (Varas, 1998).

Capítulo III. Aplicación de la metodología y desarrollo

El objetivo de este estudio es proponer un modelo para el análisis de riesgos que pueda ser implementado en la prevención de pérdida de información, enfocado al caso de estudio específico E&B promoción empresarial S.A. de C.V de tal manera que se permita delimitar funciones e identificar vulnerabilidades en áreas donde estén presentes los riesgos y para realizar esto se plantea el siguiente método:

1. Describir el problema:

Para dar inicio a la explicación de la problemática se debe conocer que la función de E&B es brindar servicios a empresas. Estos servicios son brindados en manera de proyectos los cuales son manejados por personal especializado que maneja información.

La empresa E&B promoción empresarial se encuentra en una etapa de inestabilidad debido al reciente conflicto de intereses en el manejo de dos clientes que mercadean la misma marca y el mismo producto, lo cual generó una competencia desleal por el robo y mal uso de información confidencial.

Lo cual evidencio la falta de conocimiento donde existen fugas de información y la total incapacidad para prevenirlo, motivo para tomar acciones garantizando así su seguridad en los sistemas de información.

2. Metodologías de análisis de riesgos propuestas

⁴ Se realiza una descripción de las tres metodologías posibles, las cuales se analizan: sus objetivos, pasos, procedimientos y la relación que presentan. Se tratara en un contexto de estudio y

observación, comparando la que mejor se adecue a los objetivos y necesidades principales de la empresa.

Las metodologías que se toman en cuenta son: MAGERIT, MEHARI, y la Métrica V3. Para dar inicio a la aplicación del estudio en la *tabla 1* se muestra una comparativa de los objetivos que estas metodologías manejan.

Tabla 1 Objetivo de las metodologías.

MAGERIT Ministerio de administraciones publicas (ESPAÑA)	MEHARI CLUSIF (FRANCIA)	Métrica V3
Objetivos:		
<p>Directos:</p> <ul style="list-style-type: none"> -Generar conciencia por parte de los responsables de los sistemas de información de la existencia de riesgos y la necesidad de atajarlos a tiempo. -Ofrecer un método sistemático para analizar tales riesgos -Ayudar a descubrir y planificar las medidas oportunas para mantener los riesgos bajo control. <p>Indirectos:</p> <ul style="list-style-type: none"> -Preparar a la organización para procesos de evaluación, auditoria, certificación o acreditación, según corresponda en cada caso <p>Esta metodología es de uso publico ya que no requiere una previa autorización para su uso por parte de Ministerio de Administraciones publicas de España.</p>	<p>Proporcionar un método para la evaluación y gestión de riesgos, concretamente en el dominio de la seguridad de la información, conforme a los requerimientos de la ISO/IEC 27005 :2008, proporcionando un conjunto de herramientas y elementos necesarios para su implementación.</p> <p>Indirectos:</p> <ul style="list-style-type: none"> -Permitir un análisis directo e individual de situaciones de riesgos descritas en los escenarios. -Proporcionar un completo conjunto de herramientas específicamente diseñadas para la gestión de la seguridad a corto, medio y largo plazo, adaptables a diferentes niveles de madurez y tipos de acciones considerables. 	<p>Ofrece a las organizaciones un instrumento útil para la sistematización de las actividades que dan soporte al ciclo de vida del software.</p> <p>Proporcionar o definir Sistemas de Información que ayuden a conseguir los fines de la Organización mediante la definición de un marco estratégico para el desarrollo de los mismos.</p> <ul style="list-style-type: none"> - Dotar a la Organización de productos software que satisfagan las necesidades de los usuarios dando una mayor importancia al análisis de requisitos. - Mejorar la productividad de los departamentos de Sistemas y Tecnologías de la Información y las Comunicaciones, permitiendo una mayor capacidad de adaptación a los cambios y teniendo en cuenta la reutilización en la medida de lo posible. - Facilitar la comunicación y entendimiento entre los distintos participantes en la producción de software a lo largo del ciclo de vida del proyecto, teniendo en cuenta su papel y responsabilidad, así como las necesidades de todos y cada uno de ellos. - Facilitar la operación, mantenimiento y uso de los productos software obtenidos.

Al comparar y analizar los objetivos se observa que, MAGERIT no requiere de autorización ya que es de uso público. MEHARI hace referencia de algunos requerimientos de la ISO/IEC 27005, que se pueden adecuar a los requerimientos o problemas que presente la empresa. Donde a diferencia de la metodologías anteriores la Métrica V3 es la única que se enfoca en la

sistematización de actividades que dan soporte al ciclo de vida del software.

Lo que se destaca en el análisis funcional de las metodologías, se encuentran: la gestión de riesgos, diagnóstico de seguridad, análisis de los intereses implicados por la seguridad, el análisis de riesgos, sistematización de actividades y el soporte al ciclo de vida del software. También se comparan los elementos principales que por mencionar uno por cada metodología, tenemos: la escala de valores, tabla de modelos de impactos y la gestión de proyectos, que a continuación en la *tabla 2* se muestran.

Tabla 2 Elementos principales de las metodologías.

MAGERIT Ministerio de administraciones publicas (ESPAÑA)	MEHARI CLUSIF (FRANCIA)	Métrica V3
Elementos Principales		
<ul style="list-style-type: none"> • Escalas de valores cualitativos, cuantitativos y de indisponibilidad del servicio. • Modelo de frecuencia de una amenaza como una tasa anual de ocurrencia. • Escala alternativa de estimación del riesgo. • Catálogos de amenazas. • Catálogos de medidas de control. 	<ul style="list-style-type: none"> • Niveles de categorías de controles • Niveles de calidad de los servicios de seguridad. • Evaluación de la calidad del servicio por medio de cuestionarios. • Tabla modelo de impactos. 	<ul style="list-style-type: none"> • Tipos de desarrollo: estructurado y orientado a objetos. • Gestión de proyectos • Gestión de configuración • Aseguramiento de calidad y seguridad

Hay que dejar claro que las metodologías están estructuradas en fases para poder llevarse acabo, mostradas en la *tabla 3*. Es por lo anterior que se destaca un vínculo que las relaciona siendo la determinación de los riesgos que requieren para realizar las evaluaciones, y así poder sacar las valoraciones pertinentes.

Tabla 3 Comparativa de las fases.

MAGERIT Ministerio de administraciones publicas (ESPAÑA)	MEHARI CLUSIF (CLUB DE LA SEGURIDAD DE LOS SISTEMAS DE INFORMACION DE FRANCIA)	Métrica V3
Fases		
<ol style="list-style-type: none"> 1. Identificar los activos de la empresa. 2. Determinar las amenazas. 3. Establecer las respectivas salvaguardar. 4. Estimar el impacto. 5. Determinación del riesgo. 	<ol style="list-style-type: none"> 1. Análisis de riesgos. (metodología para la elaboración del plan de seguridad). 2. Analisis sistemático de situaciones de riesgo 3. Análisis específico de situaciones de riesgo 4. Analisis de riesgo en nuevos proyectos 	Procesos de la estructura principal <ul style="list-style-type: none"> • Planificación de sistemas de información. • Desarrollo de sistemas de información. • Mantenimiento de sistemas de información.

En la *tabla 3* se muestra una comparativa de las fases de las metodologías que se puede describir de la siguiente manera, respecto a MAGERIT consta de 5 fases bien definidas y correctamente identificadas para realizar un análisis de riesgo dentro de una organización, cuyos objetivos son muy generales para cualquier tipo de organización en donde se ejecute. MEHARI se lleva a cabo en 4 pasos, que ayudan a los responsables a mantener un control y prevención sobre cualquier imprevisto o amenaza que pueda darse sobre la infraestructura de TI de una empresa, de tal forma que en el momento en el que la amenaza pase, se tomen en cuenta estas guías previamente identificadas para mitigar dichos riesgos. De manera que, métrica v3 ésta relacionada a sistemas de información de software tiene que sus fases y módulos han dado paso a la división en procesos, éstos a su vez se descomponen en actividades, y estas en tareas.

3. Determinación de los elementos metodológicos más apropiados:

Para la integración de la metodología que se implementara, se tomarán en cuenta desde sus objetivos hasta sus fases para una buena implementación en el caso de estudio. Después de comparar lo anterior se procede a decidir si se elaborara una nueva metodología o optimizar una existente. Y finalmente así realizar un análisis de riesgos en el departamento o sector de la empresa E&B que se vaya a implementar, siendo capaz de elaborar un plan de contingencia en la organización ante cualquier situación de riesgo que se presente.

Al identificar y comparar bien las fases de las metodologías se establecieron distintos criterios, ya que los nombres cambian según la situación que se presenta y en la elaboración de esta se aplicara a E&B promoción empresarial, utilizando una compilación de lo que se determinó más importante para la solución del problema. Es por lo anterior que se establecieron fases que se proponen en forma de listado:

Fases de la metodología propuesta:

1. Identificación de riesgos.
2. Evaluación de riesgos.
3. Asignación de prioridades a las aplicaciones.
4. Establecimiento de los requerimientos de recuperación.
5. Elaboración de la documentación.
6. Verificación e implementación del plan.
7. Elaboración del documento del plan de contingencia.
8. Distribución y mantenimiento del plan.

La metodología seleccionada, luego de realizar el análisis respectivo de acuerdo a las necesidades del departamento o sector de E&B promoción empresarial donde se implementará el análisis de riesgos será MAGERIT. Por que trabaja con dos partes importantes de una organización, como son la parte organizacional y la parte tecnológicas. También cuenta con fases específicas abarcando toda la información importante sin correr el riesgo de omitir datos significativos de la organización. Sin dejar pasar que será apoyada a lo largo del análisis del ciclo de contrainteligencia.

Cabe señalar que puede ser respalda con la metodología MEHARI al ser muy similar, facilitando el diagnostico del análisis tomando fases que se adecuen para una correcta implementación en la problemática del caso específico. Conviene distinguir la ventaja de la interoperabilidad que ofrece con otros actores ya que se sustentan para hacer una planeación de posibles escenarios.

4. Implementación:

Para implementar el método propuesto en el caso específico se realizó un estudio siguiendo la línea de investigación, análisis y recopilación de información, para esto es necesario llevar a cabo las fases propuestas entorno al comportamiento de la empresa. El desarrollo de la

implementación de este proyecto se dividirá en 2 partes, en este apartado se abarcará las fases iniciales que serán la introducción de los activos de la empresa y a la manera de la evaluación. Y la otra parte serán los resultados y la propuesta donde se describe las conclusiones de las evaluaciones y encuestas que se van a realizar.

Paso 1: Identificar Activos.

En este primer paso es necesario tomar en cuenta que el activo esencial de cualquier empresa es la información que maneja y que dependerá de cada empresa el valor que se le vaya a dar, todo en relación a factores como: almacenamiento, transferencia y confidencialidad entre otros. En relación a éstos factores se pueden identificar los siguientes activos de la empresa E&B:

Los servicios: se pueden prestar gracias al uso de la información que se maneja, y los servicios que se necesitan para gestionar datos son:

- Promoción directa: en esta parte se encarga de la implementación, ejecución de estrategias de promoción directa y marketing a través de personal de promoción. De igual forma realiza levantamientos y análisis de información sobre diversos factores del mercado y el consumidor con tecnología de punta. Entre los servicios que se manejan dentro de la promoción directa son: demostraciones, degustaciones, Promotoría, supervisión, merchandiser, mystery shopper, auditores de campo, volanteo, canje, track de precios, estudios de mercado, planes de lealtad y labor de venta.
- Servicios bancarios: realizan servicios de promoción y colocación de productos bancarios tales como: tarjetas de crédito (bancarias y marcas propias), créditos al consumo, tarjetas de servicio y colocación de crédito automotriz e hipotecario.
- Administración de recurso humano y reclutamiento: área encargada de la selección, capacitación, administración, supervisión, pago de nominas, operación, análisis y entrega de reportes
- Eventos y edecanes: dedicada al apoyo en la planeación, logística, coordinación y organización de eventos proporcionándoles. Aquí se enfoca al elemento humano y al

material que requieren para proyectar la imagen de sus productos o servicios.

- Apoyo promocional y alianzas estratégicas: destinada al diseño y fabricación de displays y módulos para promoción, encuestas en campo para investigación de mercados, diseño y publicidad, relaciones publicas y la división de administración de manejos de nominas.

Funciones de la organización:

- Misión: proporcionar un servicio integral de promoción para contribuir los objetivos de mercado e imagen de nuestros clientes.
- Objetivo: llegar a ser la empresa líder en promoción, brindando servicios de calidad.
- Bienes y servicios producidos: ningún bien y muchos servicios; es una empresa de promoción, administración de recurso humano.

Otros activos: los activos que maneja la empresa se pueden destacar sus herramientas de trabajo o en este caso sus software. En la *tabla 4* se muestran las aplicaciones informáticas que ayudan para la operatividad de la empresa.

Tabla 4 Aplicaciones informáticas.

APLICACIONES DE INFORMATICA	
NOMBRE	DESCRIPCION
HomeOffice	Sistema de administración de cada determinante de cada cadena comercial
• Texon	Encargado de monitorear las ventas, existencias de productos, y solicitudes de compra
• What	Imprime los artículos en pantalla de los mas vendidos, hace una comparativa de las tiendas en tiempo real
• WPIQ	Existencias de productos en el momento
Xaguar	Administración del personal, manejo de los viáticos, nominas, así como también control de faltas
Infomercados	Se encarga de monitorear el producto del respectivo proyecto en pie, y varia el funcionamiento según el enfoque del que lo ocupe

De las aplicaciones informáticas se puede destacar infomercados en la descripción nos dice que varía según el enfoque que se describe en la *tabla 5*.

Tabla 5 Infomercados según su enfoque.

Descripción infomercados según su enfoque	
Enfoque cliente externo (marca a la que se trabaja)	Enfoque cliente interno (colaboradores en este caso los líderes)
<p>El cliente puede checar como va su producto:</p> <ul style="list-style-type: none"> • El posicionamiento • Numero de ventas • El impacto • Evidencias fotográficas • Control de inventarios • Seguimiento • Toma de decisiones sobre operaciones de punto de venta • Análisis de comportamiento del mercado • Control de personal 	<p>Trabaja como:</p> <ul style="list-style-type: none"> • Una herramienta de comunicación • Checar roles • Planogramas de trabajo • Lay out • Reporteo (existencias)

Los equipos informáticos (hardware): son los activos que permiten hospedar datos, aplicaciones y servicios que utiliza el personal por cada punto de venta asignado entre ellos podemos encontrar: laptops, treo (celular), cámara fotográfica, impresora y memorias externas.

Las instalaciones: la empresa no cuenta con instalaciones fijas, todo lo hace con su personal que se encuentra laborando en los puntos de venta y se le brinda lo necesario para desempeñarse con instalaciones móviles.

El personal: parte fundamental en la empresa, se le puede considerar un activo por la capacidad que tienen en la manipulación de toda la utilería e información. Según su operatividad usan diferentes programas que a continuación se muestra en la *tabla 6*:

Tabla 6 Aplicaciones informáticas según el personal.

Manejo de aplicaciones según personal	
Tipo de personal	Programas
Coordinador regional	Todos
Coordinador local/Lideres	Infomercados, homeoffice, Xaguar
Supervisores	No maneja aplicaciones ya que todo lo que reportan es vía bitácora directamente y el líder lo sube al programa

Para una mejor comprensión del grado de confiabilidad y entender mejor la jerarquía con la cual son manejados los programas se muestra de forma detallada en la *ilustración 3*.

Ilustración 3 Distribución de la empresa.

**Dirección
general**

Subgerencia de reclutamiento y
selección

Subgerencia de capacitación

Gerencia de administración
nacional

Subgerente zona 1

Coordinadora territorial

Coordinadora local
•Supervisores

Subgerente zona 2

Coordinadora territorial

Coordinadora local
•Supervisores

Subgerente zona 3

Coordinadora territorial

Coordinadora local
•Supervisores

Gerencia de operaciones

Planeación

Compras y almacenamiento

Bancos

Control

Ejecutivo facturación

Ejecutivo mesa de control

Ejecutivo de información

Proyectos

Ejecutivo de cuenta

Ejecutivo de logística

Ejecutiva marketing

Redes de comunicaciones: entre las redes de comunicación que maneja la empresa E&B se encuentra un servidor de correo interno (ZIMBRA), este almacena toda la información o reporte de actividad que se realizó en el proceso del proyecto en pie, y OWA brinda soporte a infomercados (Telmex).

Para poder brindarle una calificación a los activos se en forma cualitativa y cuantitativa. A partir de ahí se observa un panorama más específico de las necesidades que se van presentando.

En la valoración cualitativa se determinan los siguientes factores:

- Autenticad: la pérdida de veracidad de la información.
- Confidencialidad: competencia desleal, distorsión de la información puede ser cliente externo o interno.
- Disponibilidad: lenta la comunicación y inexistencia de herramientas en el mercado para el cliente.
- Trazabilidad del uso del servicio: no habrá armonía ni dirección en toda la empresa.
- Trazabilidad de acceso de los datos: mal manejo de información producido por daños a contenidos.

Y en la valoración cuantitativa los siguientes:

- Costo de reposición: actualmente aseguran sus bienes de tal forma que lo es tangible pueda ser sustituido y lo intangible siempre este respaldado, en este caso E&B está asegurada.
- Costo de la mano de obra invertido en recuperar el valor del activo: la empresa tarda 1 semana en restaurar a nivel nacional y su costo es de \$255,140.00.
- La capacidad de operar: es invaluable ya que la operación está basada en el flujo correcto de la información y se alimenta los sistemas de información para que el cliente tenga la información de manera oportuna.

- Sanciones por incumplimiento de obligaciones contractuales: éstas equivalen al 5% del monto mensual, que paga dicho cliente por día perdido.

Paso 2: Identificar y valorar los riesgos.

Las amenazas son cosas que ocurren y en este entorno tan cambiante todo puede ocurrir, lo importante aquí es lo que pueda dañar a nuestros activos y la dimensión de dicho daño; Prevenir lo propio de los errores y permanecer alerta de las personas que colaboran de los errores o de los ataques intencionados.

4 Para determinar y valorar las amenazas que pueden afectar a cada activo se escogieron los tipos de riesgos más comunes que existen en las áreas de tecnologías de información e informática en relación a los activos que maneja la empresa, para así realizar una detallada evaluación estimando el grado de impacto y la frecuencia con la que se presenta. Entre los riesgos que se analizaron son: robo o extravío, ambientales, contaminación, integridad, relación, accesos, infraestructura, utilidad y seguridad general.

Para el análisis de la frecuencia con que se presentan las amenazas, el gerente de dicha organización propuso valores de medición de la periodicidad de uno o varios sucesos asignándole el 1 al valor con menos frecuencia y 6 al máximo que a continuación se describe la valorización y se muestra en la *tabla 7*:

- 1) NUNCA = no se presentan ningún riesgo en ningún momento.
- 2) CASI NUNCA = se ha presentado 1 vez en periodos de 5 años.
- 3) RARAS VECES = se ha presentado 1 o 2 veces al año quedando como antecedente.
- 4) ALGUNAS VECES = 1 o 2 veces por semestre.
- 5) FRECUENTEMENTE = 1 vez al mes.
- 6) SIEMPRE = todo el tiempo.

Tabla 7 Frecuencia de amenazas.

1) NUNCA - 2) CASI NUNCA - 3) RARAS VECES - 4)ALGUNAS VECES - 5) FRECUENTEMENTE - 6) SIEMPRE									
Tipo de Riesgo	Robo o extravío	Ambientales	Contaminación	Integridad	Relación	Accesos	Infraestructura	Utilidad	Seguridad general
Activo									
Servicios que prestan: Promoción Directa.									
Demostraciones									
Degustaciones									
Promotoría									
Supervisión									
Merchandiser									
Mystery Shopper									
Auditores de Campo									
Volanteo									
Canje									
Track de precios									
Estudios de mercado									
Planes de lealtad									
Labor de venta									

Para el impacto en el que se presentan las amenazas se manejaron valores del 1 (como más bajo) que no posee la suficiente capacidad; al 5 (máximo) amenaza que es altamente capaz que a continuación se describen y se muestran en la *tabla 8*:

5) ALTA = la amenaza está altamente motivada y es suficientemente capaz de llevarse a cabo.

4) MEDIA-ALTA = la amenaza está fundamentada y es posible.

3) MEDIA = la amenaza es posible.

2) MEDIA-BAJA = la amenaza no posee la suficiente capacidad.

1) BAJA= la amenaza no posee la suficiente motivación y capacidad.

Tabla 8 Impacto de las amenazas.

1) BAJO 2) MEDIO-BAJO 3) MEDIO 4) MEDIO-ALTO 5) ALTO									
Tipo de Riesgo	Robo o extravío	Ambientales	Contaminación	Integridad	Relación	Accesos	Infraestructura	Utilidad	Seguridad general
Activo									
Servicios que prestan:	Promoción Directa.								
Demostraciones									
Degustaciones									
Promotoría									
Supervisión									
Merchandiser									
Mystery Shopper									
Auditores de Campo									
Volanteo									
Canje									
Track de precios									
Estudios de mercado									
Planes de lealtad									
Labor de venta									

Para una efectiva evaluación de las amenazas se realizará un análisis detallado por cada activo según su rubro correspondiente al impacto, en el cual se detallara la relación porcentual de cada rubro creando valores exactos, lo que se busca en la tablas es darle valor fijo para tomar como base y analizar cuales serian los posibles riesgos más peligrosos. Estas tablas se mostrarán con su calificación en el apartado de los resultados.

5. Propuesta:

Se genera una solución redactando un documento donde se describan las recomendaciones del estudio que se proponen, así como también entrega de manuales y procedimientos que se hallan identificado para la resolución de las áreas de oportunidad de la empresa E&B promoción empresarial S.A. de C.V. Esta propuesta se encuentra en el apartado de anexos dirigida a los directivos de la empresa. Solo quedará como propuesta en caso de que la compañía no acceda a realizar dichos cambios en las áreas de oportunidad que se les enmarcan.

Capítulo IV. Pruebas y Resultados

En este capítulo se presenta los resultados de las entrevistas y encuestas que se llevaron a cabo al personal (directivos, puestos gerenciales y coordinadores locales) que se encuentra laborando en la empresa E&B, las cuales fueron de utilidad para valorar y calificar los activos de cada rubro tomando de manera detallada la relación de los riesgos que se puedan encontrar en la empresa.

A partir de las gráficas mostradas en el capítulo de la aplicación de la metodología, donde se describen puntualmente, se procede a la asignación de los valores en vista de los resultados de las entrevistas realizadas. De esta manera se presentan, primero en relación a la frecuencia y después en relación al impacto con la que se presentan las amenazas.

Frecuencia con la que se presentan las amenazas:

Ahora bien aclarado lo anterior, se procede a aplicar la ponderación con los resultados de las indagaciones realizadas al personal de la empresa. Comenzando con la frecuencia en la que se presentaron las amenazas, se detalla un desglose con los parámetros anteriormente descritos en las tablas que a continuación se presentan, no obstante se utiliza un sombreado para resaltar las calificaciones más relevantes que se van describiendo:

En la *tabla 7.a)* se puede observar como el personal calificó los servicios que prestan de promoción directa, con una calificación de 5 nos refiere que por lo menos 1 vez al mes los que exhiben mayor número de riesgos son las degustaciones y las demostraciones.

Tabla 7. a) Servicios de promoción directa.

1) NUNCA - 2) CASI NUNCA - 3) RARAS VECES - 4) ALGUNAS VECES - 5) FRECUENTEMENTE - 6) SIEMPRE									
Tipo de Riesgo	Robo o extravío	Ambientales	Contaminación	Integridad	Relación	Accesos	Infraestructura	Utilidad	Seguridad general
Activo									
Servicios que prestan: Promoción Directa.									
Demostraciones	2	5	5 *		5	3 *		*	*
Degustaciones	5	5	5 *		5	3 *		*	*
Promotoría	1	4	2 *		2		*	*	*
Supervisión	1	4	1 *		4		*	*	*
Merchandiser	6	5	2 *		2		*	*	*
Mystery Shopper	*	3 *		*	*	3 *		*	*
Audidores de Campo	*	4 *		*	*	*	*	*	*
Volanteo	*	4 *		*	*	*		3 *	
Canje	5	4 *		*	5		*	4	5
Track de precios	4 *	*		*	5	5 *		*	3
Estudios de mercado	2	3 *		*	*	*	*	*	*
Planes de lealtad	1 *	*		*	*	*	*	*	*
Labor de venta	1	3 *		*	*	*	*	*	*

Tabla 7. b) Servicios de promoción de Unilever.

1) NUNCA - 2) CASI NUNCA - 3) RARAS VECES - 4) ALGUNAS VECES - 5) FRECUENTEMENTE - 6) SIEMPRE									
Tipo de Riesgo	Robo o extravío	Ambientales	Contaminación	Integridad	Relación	Accesos	Infraestructura	Utilidad	Seguridad general
Activo									
Servicios que prestan: Promoción de Unilever de México									
Reclutamiento	*	5	*	*	3	*	2	*	*
Selección	*		*	*	3	*	2	*	*
Capacitación	*	5	*	*	3	*	2	*	*
Administración	*	5	*	*	4	*	3	*	3
Supervisión	*	5	*	*	3	3	3	*	3
Pago de nóminas	*	1	*	*	2	2	*	*	3
Operación	*	4	*	*	4	3	3	*	3
Análisis y entrega de reportes	4	2	*	4	4	4	2	*	4

Lo que se puede destacar de la *tabla 7.b)* relacionado a los servicios de promoción Unilever México es que existe una nula presencia en los riesgos de robo, contaminación, integridad y utilidad, por eso se califica con un asterisco por no tener algún antecedente para valorar. Al diferencia de los riesgos de acceso, seguridad general, y la integridad presentando una frecuencia

que va desde 1 o 2 veces por semestre hasta 1 o 2 veces al año quedando solo como antecedente de que se presento el riesgo.

Tabla 7. c) Servicios de apoyo promocional y alianzas estratégicas.

1) NUNCA - 2) CASI NUNCA - 3) RARAS VECES - 4) ALGUNAS VECES - 5) FRECUENTEMENTE - 6) SIEMPRE									
Tipo de Riesgo	Robo o extravío	Ambientales	Contaminación	Integridad	Relación	Accesos	Infraestructura	Utilidad	Seguridad general
Activo									
Servicios que prestan: Apoyo promocional y alianzas estratégicas.									
Diseño y fabricación de displays y módulos para promoción	2	3	1	1	3	1	3	2	2
Encuestas en campo para investigación de mercados	2	4	1	1	3	1	1	*	*
Diseño y publicidad	3	4	1	1	2	1	1	*	*
Diseño y confección de uniformes	1	*	*	*	1	*	*	*	4
Relaciones Publicas	1	*	*	*	2	*	*	*	*
División de administración y manejos de nominas	2	*	*	2	3	1	1	1	3

De cierta manera en lo que se refiere los servicios de apoyo promocional y alianzas estratégicas en la *tabla 7.c)* se muestra la poca frecuencia que se presentan los riesgos menores a 1 o 2 veces por semestre con una calificación de 1. Los que riesgos que resaltan por que presentan un riesgo mínimo son: contaminación, integridad e infraestructura.

Tabla 7. d) Aplicaciones informáticas (Software).

1) NUNCA - 2) CASI NUNCA - 3) RARAS VECES - 4) ALGUNAS VECES - 5) FRECUENTEMENTE - 6) SIEMPRE									
Tipo de Riesgo	Robo o extravío	Ambientales	Contaminación	Integridad	Relación	Accesos	Infraestructura	Utilidad	Seguridad general
Activo									
Aplicaciones informáticas (Software)									
Homeoffice	3	1	*	1	5	4	1	2	5
Texon	4	1	*	2	6	3	2	2	5
What	3	1	*	3	6	3	2	2	5
WPIQ	2	1	*	3	5	3	2	2	*
Xaguar									
Administración de personal	5	1	*	5	5	4	4	4	*
Viáticos	4	1	*	4	6	4	5	5	*
Nominas	4	1	*	3	6	4	4	4	*

En cuanto a los programas informáticos que maneja el personal de la empresa, se distingue que el riesgo con la calificación máxima con 6 en algunos activos infiere que se presentan todo el tiempo fue, el uso no oportuno de la información (relación). Al mismo tiempo se muestran riesgos con una calificación de 5 que manifiestan una frecuencia de por lo menos 1 vez al mes, por lo que se puede destacar de la *tabla 7.d*).

Tabla 7. e) Aplicaciones informáticas: infomercados externo.

Tipo de Riesgo	Robo o extravío	Ambientales	Contaminación	Integridad	Relación	Accesos	Infraestructura	Utilidad	Seguridad general
Activo									
Aplicaciones informáticas (Software)									
Infomercados enfoque Externo									
Ventas	4	4	*	3	4	4	5	3	4
Posicionamiento	2	4	*	3	4	2	5	3	4
Impacto	4	4	3	4	4	2	4	4	4
Evidencias fotográficas	5	4	2	3	5	4	5	3	5
Control de inventarios	5	4	2	4	5	4	4	4	5
Seguimientos	4	4	2	3	5	4	3	3	4
Toma de decisiones sobre operaciones de punto de venta	3	3	*	2	2	2	2	2	2
Análisis de comportamiento del mercado	4	4	*	2	2	2	1	2	3
Control de personal	5	4	*	2	*	2	1	2	3

Tabla 7. f) Aplicaciones informáticas: infomercados interno.

1)NUNCA - 2) CASI NUNCA - 3) RARAS VECES - 4)ALGUNAS VECES – 5)FRECUENTEMENTE – 6)SIEMPRE									
Tipo de Riesgo	Robo o extravío	Ambientales	Contaminación	Integridad	Relación	Accesos	Infraestructura	Utilidad	Seguridad general
Activo									
Aplicaciones informáticas (Software)									
Infomercados enfoque Interno									
Herramienta de comunicación	2	2	3	4	5	4	4	4	3
Chequeo de roles	3	4	*	4	5	4	5	3	4
Planogramas de trabajo	3	3	*	4	5	5	4	4	4
Lay out	4	3	*	5	5	5	5	4	4
Reporteo (Existencias)	5	4	*	5	*	5	5	5	5

De acuerdo con las tablas de software de infomercados en sus enfoques tanto externo como interno presentadas en las *tablas 7.e) y 7.f)*, se observa una frecuencia en los riesgos mayores a 1 o 2 veces por semestre y en algunos casos 1 vez al mes, aclarando que existe una mayor periodicidad en lo que infomercados por la relación que existe entre el personal y software.

Tabla 7. g) Equipos informáticos (hardware), instalaciones y redes de comunicaciones.

1) NUNCA - 2) CASI NUNCA - 3) RARAS VECES - 4) ALGUNAS VECES - 5) FRECUENTEMENTE - 6) SIEMPRE									
Tipo de riesgo	Robo o extravío	Ambientales	Contaminación	Integridad	Relación	Accesos	Infraestructura	Utilidad	Seguridad general
Activo									
Servicios que prestan: Equipos informáticos (hardware)									
Laptops	4	2	5	5	5	4	3 *		3
Smartphone	6	4	2	6	5	2	4 *		2
Cámara fotográfica	3	2	2	6	5	1	2 *		1
Impresora	2	2	5	6	5	1	1 *		3
Memorias Externas (HD)	4	3	3	6	5	5	1 *		1
Servicios que prestan: Instalaciones									
Instalaciones móviles	3	3	2	6	2	3	3 *		2
Redes de comunicaciones									
Servidor de correo interno(Zimbra)	4	1	1	6	3	5	2 *		1
Soporte a infomercados (OWA)	1	2	1	3	2	2	1 *		1

Con respecto a los equipos informáticos en la *tabla 7.g)*, se observa a la integridad con el riesgo que tiene mayor frecuencia por su calificación de 6, esto es por que involucra al personal con uso de información sin autorización con una periodicidad de todo el tiempo en la mayoría de los activos. También que los riesgos de robo/extravío, relación y accesos destacan una puntuación recurrente desde 1 o 2 veces por semestre hasta 1 vez al mes.

De acuerdo a las ponderaciones presentadas en las tablas anteriores se realizó una serie de operaciones matemáticas resumidas en la fórmula siguiente:

$$x = \frac{cr}{(tr \times cm)} \dots\dots\dots [Fórmula 1]$$

Donde:

cr= suma total de las calificaciones recolectadas,

tr= el numero total de rubros que contiene el servicio que presta (dependerá de cada servicio),

cm= calificación máxima.

x= porcentaje final de las evaluaciones de cada activo

Conviene distinguir que se realizo esa misma operación a todos los riesgos presentados en la *tabla 9* y se definió al 100% como máximo grado de frecuencia en la que se presento el riesgo.

Ej. $28/(13 \times 6) = 35.90$

Tabla 9 Concentrado general de frecuencia de amenazas.

Tipo de riesgo Activo	Robo o extravío	Ambientales	Contaminación	Integridad	Relación	Accesos	Infraestructura	Utilidad	Seguridad general
Promoción Directa.	35.90	56.41	19.23	0.00	35.90	17.95	0.00	8.97	10.26
Promoción de Unilever de México	8.33	56.25	0.00	8.33	54.17	25.00	35.42	0.00	33.33
Eventos y edecanes	0.00	53.33	0.00	0.00	50.00	0.00	63.33	0.00	66.67
Apoyo promocional y alianzas estratégicas.	30.56	30.56	9.44	13.89	38.89	11.11	16.67	8.33	13.89
Aplicaciones informáticas (Software)	50.00	16.67	0.00	37.50	91.67	54.17	29.17	33.33	62.50
Xaguar	54.44	16.67	0.00	66.67	94.44	66.67	72.22	72.22	0.00
Infomercados Enfoque Externo	66.67	64.81	16.67	48.15	57.41	48.15	55.56	48.15	62.96
Infomercados Enfoque Interno	56.67	53.33	10.00	73.33	66.67	76.67	76.67	66.67	66.67
informáticos (hardware)	63.33	43.33	56.67	96.67	83.33	43.33	36.67	0.00	33.33
Instalaciones móviles	50.00	50.00	33.33	100.00	33.33	50.00	50.00	0.00	33.33
Redes de comunicaciones	41.67	25.00	16.67	75.00	41.67	58.33	25.00	0.00	16.67

De la misma manera para la evaluación de las amenazas se realizaron operaciones matemáticas para ubicarlas según su porcentaje de riesgo. Para esto se empleo la siguiente fórmula:

$$Pr = \frac{tr \times mp}{s} \dots\dots\dots [Fórmula 2]$$

Donde:

tr= suma del numero de tipos riesgos,

mp= valor del máximo porcentual

s= suma total de los valores que se le asignaron a los riesgos suponiendo que 100 sea el máximo por cada riesgo.

pr= porcentaje de riesgo

Tabla 10 Evaluación de la susceptibilidad de los activos.

Evaluacion de las amenazas	
Activo	% de riesgo
Promoción Directa.	21%
Promoción de Unilever de México	25%
Eventos y edecanes	26%
Apoyo promocional y alianzas estratégicas.	19%
Aplicaciones informáticas (Software)	42%
Xaguar	49%
Infomercados Enfoque Externo	52%
Infomercados Enfoque Interno	61%
Equipos informáticos (hardware)	51%
Instalaciones móviles	44%
Redes de comunicaciones	33%

En la etapa de evaluación de amenazas se aplicó la *fórmula 2* en promoción directa para sacar el porcentaje de riesgo, quedando de la siguiente manera: $9 \times 100\% / 900 = 21\%$. Donde se utilizó en el caso de todos los activos evaluados y se concluye que los que presentaron mayor frecuencia en relación a las amenazas son:

1. Software de infomercados (enfoque interno).
2. Software de infomercados (enfoque externo).
3. Dentro de los servicios que prestan, los equipos informáticos.
4. Software de Xaguar.

Descrito lo anterior es bueno señalar que la *tabla 10* se destaca el activo con mayor riesgo el de infomercados interno por ser el encargado de monitorear el producto del respectivo proyecto en pie, también sirve como herramienta de comunicación. En cuanto a la accesibilidad involucra al personal con el uso de la información lo cual implica un riesgo latente .

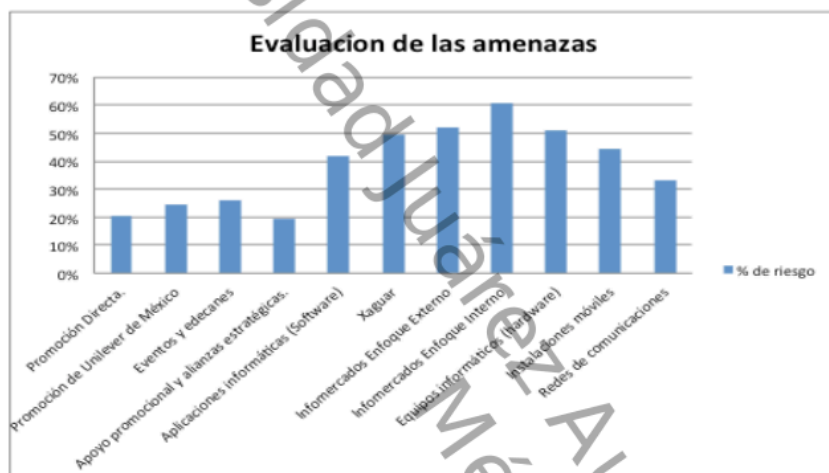


Ilustración 4 Gráfica de la susceptibilidad del activo.

Por otro lado el activo con una calificación menor de la *ilustración 4* es el apoyo promocional, puesto que sus funciones son las relaciones públicas, encargado de el diseño y la publicidad lo cual no genera un riesgo mayor por el tipo de información que se maneja.

Para una mejor comprensión del fenómeno se analizó la frecuencia que se presentan los riesgos por lo tanto los que indican mayores efectos son:

- Relación.
- Integridad.
- Ambientales.
- Infraestructura.



Ilustración 5 Gráfica de los niveles porcentuales según el tipo de riesgo.

De este modo se puede concluir de la *ilustración 5* el riesgo con mayor frecuencia es la relación, por que los empleados mencionan tener constantemente problemas con el uso no oportuno de la información. A diferencia de la contaminación que es el que menor repercute ya que no afectan a gran en medida.

Impacto de las amenazas con las que se presentan:

Ahora bien en este apartado se califico a los activos según el grado en el que son afectados los activos de la empresa para ello, se realizo con ayuda del personal que labora una serie de ponderaciones que se muestran en las siguientes tablas que de igual manera se fueron resaltando por medio de sombreados las casillas que fueron sobresaliendo:

Tabla 8. a) Servicios de promoción directa

1) BAJO 2) MEDIO-BAJO 3) MEDIO 4) MEDIO-ALTO 5) ALTO									
Tipo de Riesgo	Robo o extravío	Ambientales	Contaminación	Integridad	Relación	Accesos	Infraestructura	Utilidad	Seguridad general
Activo									
Servicios que prestan: Promoción Directa.									
Demostraciones	5	4	3	5	5	5 *		5	5
Degustaciones	5	5	5	5	5	5 *		4	5
Promotoría	4	4	3	5	5	5 *		3	3
Supervisión	3	4	2	5	5	5 *		3	5
Merchandiseo	5	5	2	4	4	4 *		4	4
Mystery Shopper	3	4	2	4	5	5 *		4	3
Audidores de Campo	5	4	2	3	4	4 *		5	5
Volanteo	4	4	2	3	4	4 *		4	3
Canje	5	4 *		2	4	3 *		3	4
Track de precios	5	4	1	5	5	5 *		5	5
Estudios de mercado	5	5	3	4	5	4 *		5	4
Planes de lealtad	4	4	2	2	4	5 *		4	3
Labor de venta	*	3 *		3	5	5 *		3	3

Examinando la *tabla 8.a)* se puede destacar que existe alto grado de impacto en la promoción directa que maneja la empresa, por su valioso contenido de información en los activos, presentándose en su gran mayoría una puntuación arriba de 4, que indica la existencia de una posible amenaza ya fundamentada y que es altamente motivada a efectuarse.

Tabla 8. b) Servicios de promoción Unilever.

1) BAJO 2) MEDIO-BAJO 3) MEDIO 4) MEDIO-ALTO 5) ALTO									
Tipo de Riesgo	Robo o extravío	Ambientales	Contaminación	Integridad	Relación	Accesos	Infraestructura	Utilidad	Seguridad general
Activo									
Servicios que prestan: Promoción de Unilever de México									
Reclutamiento	*	4	2	4	4	5	4	3	5
Selección	*	4	2	4	4	5	5	2	5
Capacitación	5	5	2	4	5	5	5	5	5
Administración	5	5	2	5	5	5	5	5	5
Supervisión	5	4	2	3	5	5	5	3	2
Pago de nóminas	5	5	2	5	5	5	5	5	5
Operación	5	5	2	5	5	5	5	5	5
Análisis y entrega de reportes	5	4	2	5	5	5	5	5	5

Ahora en concordancia a la promoción de Unilever se percibe una ponderación alta en los activos en general ya que son propensos a que afecte con mayor riesgo, a diferencia de la contaminación que es el único activo no genera mayor impacto peligro ya que la amenaza no posee la suficiente capacidad para presentarse con una calificación de medio-bajo.

Tabla 8. c) Servicios de eventos y edecanes.

1) BAJO 2) MEDIO-BAJO 3) MEDIO 4) MEDIO-ALTO 5) ALTO									
Tipo de Riesgo	Robo o extravío	Ambientales	Contaminación	Integridad	Relación	Accesos	Infraestructura	Utilidad	Seguridad general
Activo									
Servicios que prestan: Eventos y edecanes									
Planeación	2	1	*	4	5	5	4	5	4
Logística	3	5	*	4	5	5	5	5	5
coordinación	4	2	*	4	5	5	5	4	5
Organización	4	5	*	5	5	5	5	5	5
Material publicitario	5	4	*	5	2	5	3	2	3

Por lo que respecta al servicio de edecanes refleja los riesgos que más afectan son la relación, accesos y la infraestructura no obstante el activo que muestra mayor impacto es la organización ya que le afectan en su totalidad los tipos de riesgos que se le calificaron.

Tabla 8. d) Servicios de apoyo promocional y alianzas estratégicas.

1) BAJO 2) MEDIO-BAJO 3) MEDIO 4) MEDIO-ALTO 5) ALTO									
Tipo de Riesgo	Robo o extravío	Ambientales	Contaminación	Integridad	Relación	Accesos	Infraestructura	Utilidad	Seguridad general
Activo									
Servicios que prestan: Apoyo promocional y alianzas estratégicas.									
Diseño y fabricación de displays y módulos para promoción	5	3	1	5	5	5	5	5	4
Encuestas en campo para investigación de mercados	5	3	1	5	5	5	5	5	5
Diseño y publicidad	5	3	1	5	5	5	5	5	5
Diseño y confección de uniformes	3	3	1	1	1	2	1	1	3
Relaciones Publicas	1	*	1	1	2	2	1	1	5
División de administración y manejos de nominas	5	3	1	5	5	5	5	5	5

Ahora analizando el apoyo promocional y alianzas estratégicas de la *tabla 8.d)* se observa que el riesgo de contaminación no posee la suficiente capacidad para afectar, aunque de lado de los activos los que presentaron menor impacto fueron las relaciones publicas y confección de uniformes.

Tabla 8. e) Aplicaciones informáticas.

1) BAJO 2) MEDIO-BAJO 3) MEDIO 4) MEDIO-ALTO 5) ALTO									
Tipo de Riesgo	Robo o extravío	Ambientales	Contaminación	Integridad	Relación	Accesos	Infraestructura	Utilidad	Seguridad general
Activo									
Aplicaciones informáticas (Software)									
Homeoffice	5	5	5	2	5	5	4	4	5
Texon	5	5	5	2	5	5	4	3	5
What	5	5	5	2	5	5	4	3	5
WPIQ	5	5	5	2	5	5	4	3	5
XAGUAR									
Administración de personal	5	5	2	5	5	5	5	5	5
Viáticos	5	5	2	5	5	5	5	5	5
Nominas	5	5	2	5	5	5	5	5	5

Tabla 8. f) Aplicaciones informáticas: infomercados externo.

1) BAJO 2) MEDIO-BAJO 3) MEDIO 4) MEDIO-ALTO 5) ALTO									
Tipo de Riesgo	Robo o extravío	Ambientales	Contaminación	Integridad	Relación	Accesos	Infraestructura	Utilidad	Seguridad general
Activo									
Aplicaciones informáticas (Software)									
Infomercados enfoque externo									
Ventas	5	4	*	5	5	5	5	5	5
Posicionamiento	5	4	*	1	3	5	5	5	2
Impacto	3	4	*	1	5	3	5	5	2
Evidencias fotográficas	5	3	*	5	3	5	5	5	5
Control de inventarios	5	5	*	5	5	5	5	5	5
Seguimientos	5	5	*	5	5	5	5	5	5
Toma de decisiones sobre operaciones de punto de venta	2	5	*	4	5	2	4	5	3
Análisis de comportamiento del mercado	1	5	*	2	2	1	3	5	3
Control de personal	5	5	*	5	4	5	2	5	5

Tabla 8. g) Aplicaciones informáticas: Infomercados interno.

1) BAJO 2) MEDIO-BAJO 3) MEDIO 4) MEDIO-ALTO 5) ALTO									
Tipo de Riesgo	Robo o extravío	Ambientales	Contaminación	Integridad	Relación	Accesos	Infraestructura	Utilidad	Seguridad general
Activo									
Aplicaciones informáticas (Software)									
Infomercados enfoque interno									
Herramienta de comunicación	5	2	1	5	5	5	5	5	5
Chequeo de roles	5	4	*	5	5	5	5	5	5
Planogramas de trabajo	5	4	*	5	5	5	5	5	5
Lay out	4	4	*	5	5	5	5	5	5
Reporteo (Existencias)	4	4	*	5	5	5	5	5	5

En suma de las calificaciones obtenidas sobre los programas informáticos que utiliza la empresa mostradas en las *tablas 8.e)-8.g)*, es claro que la cantidad de información que se manejan en estos activos es relevante con una calificación en su gran mayoría de 5, reflejando un alto grado en el impacto de las amenazas por la cantidad de datos que se procesa con su uso diario.

Tabla 8. h) Equipos informáticos (hardware), instalaciones y redes de comunicaciones.

1) BAJO 2) MEDIO-BAJO 3) MEDIO 4) MEDIO-ALTO 5) ALTO									
Tipo de riesgo	Robo o extravío	Ambientales	Contaminación	Integridad	Relación	Accesos	Infraestructura	Utilidad	Seguridad general
Activo									
Servicios que prestan: equipos informáticos (hardware)									
Laptops	5	3	1	5	2	5	5	5	5
Smartphone	5	1	1	5	3	5	5	5	5
Cámara fotográfica	3	1	1	*	*	2	*	1	2
Impresora	2	1	1	*	*	2	*	*	2
Memorias Externas (HD)	5	1	1	5	5	5	1	5	5
Servicios que prestan: instalaciones									
Instalaciones móviles	5	5	1	5	5	1	2	5	*
Redes de comunicaciones									
Servidor de correo interno (Zimbra)	1	1	*	5	5	5	5	5	5
Soporte a infomercados (OWA)	1	1	*	5	5	5	5	5	5

Derivado de esto, se muestra la calificación del impacto que presentaron los hardware, instalaciones y las redes de comunicaciones. En síntesis, dependiendo en donde sea empleada la información más severo será el impacto de las amenazas por citar un ejemplo de la *tabla 8.h*) las laptops es el activo que más sobresale por la utilidad diaria que se le brinda en la empresa.

Tabla 11 Concentrado general del impacto del riesgo.

1)BAJA 2)MEDIA-BAJA 3)MEDIA 4)MEDIA-ALTA 5)ALTA									
Tipo de riesgo	Robo o extravío	Ambientales	Contaminación	Integridad	Relación	Accesos	Infraestructura	Utilidad	Seguridad general
Activo									
Promoción Directa.	81.54	83.08	41.54	76.92	92.31	90.77	0.00	80.00	80.00
Administración de Recursos Humanos	75.00	90.00	40.00	87.50	95.00	100.00	97.50	82.50	92.50
Eventos y edecanes	72.00	68.00	0.00	88.00	88.00	100.00	88.00	84.00	88.00
Apoyo promocional y alianzas estratégicas.	80.00	50.00	20.00	73.33	76.67	80.00	73.33	73.33	90.00
Aplicaciones informáticas (Software)	100.00	100.00	40.00	100.00	100.00	70.00	80.00	65.00	100.00
Xaguar	100.00	100.00	40.00	100.00	100.00	100.00	100.00	100.00	100.00
Infomercados Enfoque Externo	75.56	88.89	0.00	73.33	82.22	80.00	86.67	100.00	77.78
Infomercados Enfoque Interno	92.00	72.00	4.00	100.00	100.00	100.00	100.00	100.00	100.00
Equipos informáticos (hardware)	80.00	28.00	20.00	60.00	40.00	76.00	44.00	64.00	76.00
Instalaciones móviles	100.00	100.00	20.00	100.00	20.00	40.00	100.00	0.00	40.00
Redes de comunicaciones	100.00	100.00	20.00	100.00	20.00	40.00	100.00	0.00	40.00

Aquí he de referirme, que para la obtención de los resultados presentados en la *tabla 11* se realizó de igual forma que en las frecuencias, se empleo la *Fórmula 1* para ubicar el porcentaje del impacto del riesgo en las amenazas; Ej.: $53/(13*5)=81.54$, donde 53 es la suma total de las valoraciones del riesgo, 13 es el número total de los rubros que contiene el servicio que presta (dependerá de cada servicio), 5 es la calificación máxima que se propuso.

Tabla 12 Evaluación de las amenazas que impactan a los activos.

Evaluación de impacto	
Activos	% de riesgo
Xaguar	93%
Infomercados Enfoque Interno	85%
Administración de Recursos Humanos	84%
Aplicaciones informáticas (Software)	84%
Eventos y edecanes	75%
Infomercados Enfoque Externo	74%
Promoción Directa.	70%
Apoyo promocional y alianzas estratégicas.	69%
Instalaciones móviles	58%
Redes de comunicaciones	58%
Equipos informáticos (hardware)	54%

De acuerdo con el concentrado general de impacto de amenazas, para una mejor evaluación se muestra la *tabla 12* donde se determina su porcentaje de riesgo por medio de la *fórmula 2*, antes aplicada con las frecuencias. Para conocer su valor porcentual y presentar cuales son las más peligrosas o que generan mayor impacto para la empresa. Llegado a este punto es bueno destacar que los activos con alto grado de impacto por arriba del 75% evaluados en relación a los riesgos presentados son:

- 1.- Software: Xaguar.
- 2.- Aplicaciones informáticas: infomercados según su enfoque interno.
- 3.- Servicios que prestan: administración de recursos humanos.
- 4.- Eventos y edecanes.

Al mencionar a Xaguar como uno de los activos con mayor impacto de amenazas se debe a que es el programa que se encarga de la administración del personal, del manejo de viáticos, nominas y control de asistencias. Si llegara a fallar este programa repercutiría en gran medida en la productividad de la empresa por que entra en relación directa con el personal de la empresa y los datos.

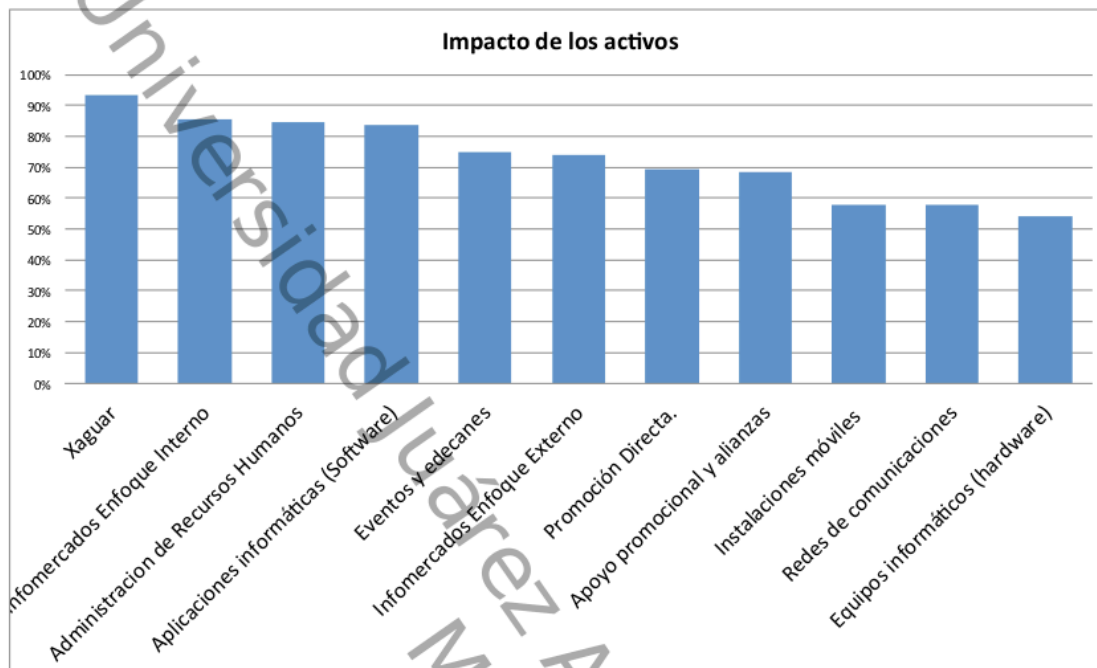


Ilustración 6 Gráfica del porcentaje de impacto en los activos.

Para ello en la *ilustración 6* muestra una gráfica del impacto, donde se observa como la tendencia hacia los programas informáticos afecta de manera relevante ya que son de suma importancia para la operatividad de ciertos activos causando un riesgo inminente y esto es debido al tipo de información que se maneja a como se ha venido comentando. A diferencia de los hardware o las instalaciones físicas que tienden a ser un poco menor pero sus porcentajes llegan a tener ese valor que se hace visible que no se debe dejar a un lado.

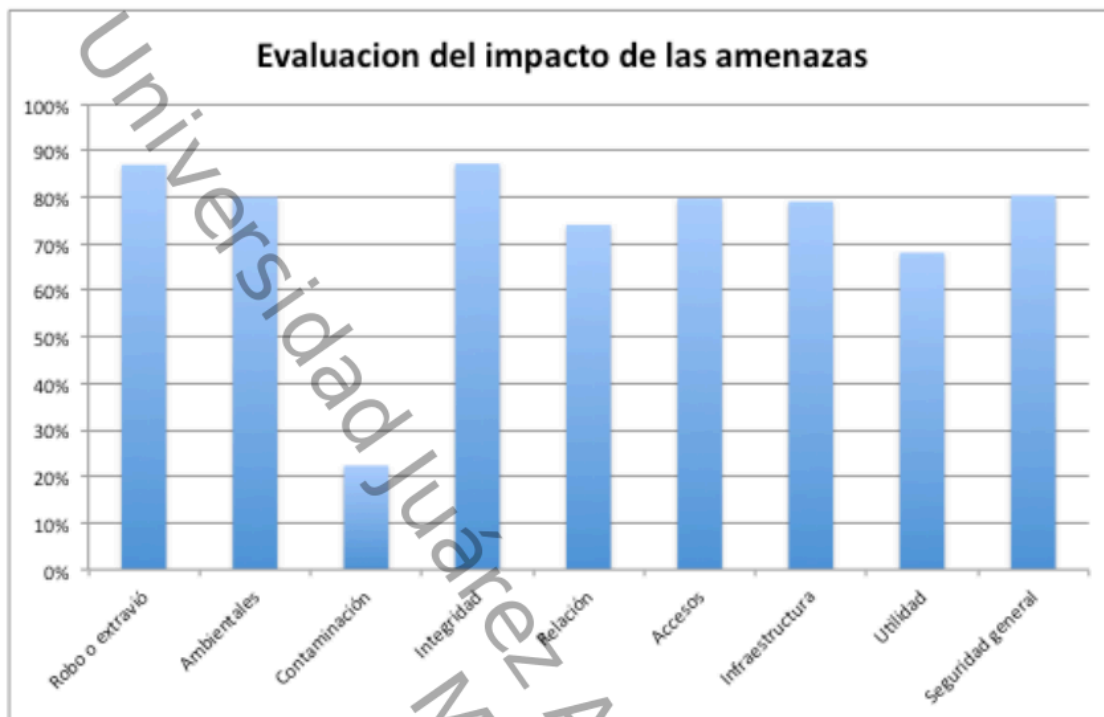


Ilustración 7 Gráfica de las amenazas según su impacto.

Al respecto conviene destacar que en la *ilustración 7* las amenazas que más impactan por arriba del 85% son:

- 1.- La integridad.
- 2.- Robo o extravío.
- 3.- Seguridad General.
- 4.-Cuestiones Ambientales.
- 5.- Acceso.

Para comprender la importancia del impacto en la integridad, es por que se encarga de los riesgos que involucran al personal con uso de información sin autorización y las restricciones es decir se encuentran con un pobre mantenimiento en el área de sistemas. Por lo contrario la gráfica de amenazas ubica a la contaminación con menor impacto esto es, a decir de los empleados no han

tenido problemas que hallan afectado en gran medida con la información para generar una preocupación al respecto.

Para finalizar con el análisis de riesgos realizado, se ha clasificado los tres primeros activos en orden de mayor a menor grado, según la prioridad que se consideraron más importantes y que se sugiere tener un mayor control de los riesgos ya sea el caso de la frecuencia en la *tabla 13* o del impacto en la *tabla 14*:

Tabla 13 Compendio de la frecuencia de los riesgos

Riesgos con mayor frecuencia:			
1. Infomercados (interno)			
	Acceso	Infraestructura	Integridad
1ro	Planogramas de trabajo	Chequeo de roles	Reporteo
2ndo	Lay out	Lay out	Lay out
3ro	Reporteo	Reporteo	Herramientas de comunicación
2. Infomercados (externo)			
	Robo o extravió	Ambiental	Seguridad general
1ro	Evidencias fotográficas	Control de inventarios	Evidencia
2ndo	Control de inventarios	Control de personal	Control de inventarios
3ro	Control de personal	Evidencias fotográficas	Ventas
3. Equipos de información (hardware)			
	Integridad	Relación	Robo o extravió
1ro	Smartphone	Laptops	Smartphone
2ndo	Laptops	Smartphone	Laptops
3ro	Memorias o DD	Cámara fotográfica	Memorias o DD

Tabla 14 Compendio del impacto de riesgos

Riesgos con mayor impacto:			
Xaguar			
	Integridad	Seguridad general	Relación
1ro	Administración de personal	Administración de personal	Administración de personal
2ndo	Viáticos	Viáticos	Viáticos
3ro	Nominas	Nominas	Nominas
Infomercados (interno)			
	Integridad	Relación	Acceso
1ro	Herramientas de comunicación	Herramientas de comunicación	Herramientas de comunicación
2ndo	Planogramas de trabajo	Lay out	Chequeo de roles
3ro	reporteo	Reporteo	Lay out
Administración de recursos humanos			
	Acceso	Infraestructura	Seguridad general
1ro	Capacitación	Capacitación	Capacitación
2ndo	Administración	Administración	Administración
3ro	Supervisión	Supervisión	Supervisión

Llegado a este punto es bueno mencionar que se incluye una propuesta en el apartado de anexos donde se describen los puntos con mayor impacto y frecuencia que tienen los activos, adjunto con una serie de recomendaciones para su mejor desempeño ante los problemas que se han suscitado con anterioridad. Lo que ayudara a llevar a un correcto manejo con los activos de la empresa y así una mejora en su seguridad de la información para escenarios futuros desde el punto de vista del análisis presentado.

Capítulo V. Conclusiones y trabajos futuros

5.1 Conclusiones

Con las consideraciones anteriores fundamentan la propuesta para el análisis de un modelo de prevención de riesgos en la seguridad de información, arrojando como resultado que E&B Promoción Empresarial S.A. de C.V. actualmente cuenta con áreas de oportunidad que requieren ser reforzada. Mostrando un alto manejo de información con bajos requerimientos de seguridad establecidos, siendo así propensos a numerosas pérdidas de sus activos más importantes.

De acuerdo a la problemática presentada se planteó la siguiente pregunta: ¿Que características en el manejo de la información permite definir un modelo apropiado para garantizar la seguridad de la información de la empresa E&B promoción empresarial?

Para tener una perspectiva más detallada, se propuso un análisis donde se detectaron los riesgos de seguridad en la información para la empresa E&B, que permitió implementar un modelo apropiado con los controles, procedimientos y herramientas para la prevención de pérdida de información, apoyándose del ciclo de contra-inteligencia.

Este estudio proporcionó una mejor estabilidad en el campo competitivo de las empresas de hoy en día. Donde se fortaleció la relación de áreas informáticas, información y de personal con una comunicación efectiva y una planeación apropiada.

Se realizó un estudio exhaustivo de la información sobre 3 metodologías propuestas, que mostraron las diferencias, fortalezas y debilidades en relación al caso en particular que se presentó. Por ello se llegó a la conclusión de usar la metodología MAGERIT como pilar fundamental para el análisis de riesgos de la seguridad de la información amparado con a la metodología MEHARI, ya que tienen similitudes en sus objetivos. Además proporciona la

facilidad de ser compatible con otros tipos de giros empresariales siempre y cuando se desee mejorar la seguridad de la información.

En cuanto a los beneficios del uso de esta propuesta para las empresas, se considera que tiene una relevancia significativa en el área de la seguridad, ya que permite tener un mejor control del manejo de la información en relación con la gente que la manipula. Esto se percibe por el tiempo y el gasto económico que la empresa requiere para sobrellevar ciertos acontecimientos no gratos afectándoles directamente en su productividad.

Con el uso de la metodología propuesta se pretende que las empresas mexicanas generen conciencia que la información es su activo primordial y que al ser sustraído intencionadamente o sin darse cuenta, genera un riesgo el cual muchas empresas no están dispuestas a darse el lujo de caer en ella. Es por ello que con una serie de procedimientos se genera un beneficio por tener la interoperabilidad con otras empresas ya que se puede manejar desde un ámbito de prevención de riesgo hasta cuando la amenaza ya halla generado algún efecto.

5.2 Trabajos futuros

Derivado de la propuesta que se plantea en este proyecto se describen algunas actividades y sugerencias para darle un seguimiento al análisis de riesgos de la seguridad de la información en base a las metodologías ya estudiadas y a su aplicación en las PyMES la continuidad del estudio radicará en:

- El diseño de una matriz de análisis con n variables sobre el estado actual de x empresa.
- Donde los resultados arrojados se clasificarán de acuerdo a una semaforización de riesgos en impactos.
- Una vez identificados se realizará la adecuación de estas metodologías más otras que no se estudiaron para garantizar que las empresas u organizaciones estén realizando las mejores prácticas.

- Desarrollar un tablero de control y toma de decisiones donde los niveles directivos puedan consultar y elegir del abanico de soluciones planteando la que consideren optima.
- Diseñar un sistema de gestión que le permita garantizar la confidencialidad, integridad y disponibilidad, de la información, los servicios de consulting en el análisis de riesgos se deben adecuar de acuerdo al giro de la organización y dependiendo de los productos /o servicios.
- Buscar alianzas estratégicas en desarrollo para generar como proteger las PyMES.
- Realizar de un software que se cree a partir de el análisis de metodologías de análisis de riesgos para calificar de manera automática empresas de manera eficiente.

Capítulo VI. Bibliografía

- CCN- Cert Seguridad TiC. (2011). *Centro Criptológico Nacional en Madrid*. Retrieved 2011 йил 22-Marzo from www.ccn-cert.cni.es: www.ccn-cert.cni.es
- CCN- Cert Seguridad TiC. (2007 йил 24-Abril). (CCN- Cert) Retrieved 2011 йил 22-03 from CCN- Cert Capacidad de respuesta ante incidentes de seguridad de red: https://213.192.250.94/index.php?option=com_content&view=article&id=1577%3AAlas-amenazas-y-vulnerabilidades-sobre-los-sistemas-de-informacion-se-incrementaron-un-55&catid=62%3Acomunicados-ccn-cert&Itemid=86&lang=es
- Campos, J. G. (15 de Septiembre de 2004). *Mailxmail*. Obtenido de <http://www.mailxmail.com/>: <http://www.mailxmail.com/curso-delitos-informaticos/impacto-nivel-social>
- Cardoso Jr, W. F. (Noviembre de 2007). Contrainteligencia Empresarial. *AA inteligencia* .
- Comai, A. (2003). La contrainteligencia. . *PUZZLE: Revista Hispana de la Inteligencia Competitiva* . , 7, 3-5.
- Corti, M. E. (24 de Julio de 2010). Hacia una implementación exitosa de un SGSI. *Metodologías para la implantación de SGSI* .
- Symantec. (2009 йил 5-Noviembre). *Tecnología PYME*. Retrieved 2011 йил 03-Marzo from www.tecnologiapyme.com: <http://www.tecnologiapyme.com/software/symantec-data-loss-prevention-seguridad-para-los-datos-confidenciales>
- Spanishpmo. (19 de Abril de 2009). *Spanishpmo*. Recuperado el 22 de Marzo de 2011, de spanishpmo.com: <http://spanishpmo.com/index.php/que-es-seguridad-de-la-informacion/>
- Soto, L. (2008). *Mi Tecnológico*. Recuperado el 22 de Marzo de 2011, de [mitecnologico.com](http://www.mitecnologico.com): <http://www.mitecnologico.com/Main/SeguridadLogicaYConfidencial>

- Soto, L. (Noviembre de 2009). *Mi tecnológico*. Recuperado el 20 de marzo de 2010, de Mi tecnológico: <http://www.mitecnologico.com/Main/TiposDeInformacion>
- Unisul, T. E. (2005). *Inteligência empresarial estratégica: método de implantação de inteligência competitiva em organizações*. Brazil: Tubarão: Editora da Unisul.
- Vanaclocha, P. (29 de Marzo de 2009). Errores comunes en la Implantación de un SGSI. *Security artwork*.
- Varas, A. (1998). *Aritmética y geometría práctica de la Real Academia de San Fernando*. . En la imprenta de la viuda de Ibarra. ed (en español).
- Talens-Oliag, S. (2009). *Instalación y configuración segura de sistemas Unix*. Recuperado el 22 de Marzo de 2011, de [www.uv.es](http://www.uv.es/~sto/cursos/icssu/html/ar01s04.html): <http://www.uv.es/~sto/cursos/icssu/html/ar01s04.html>
- Tecnologia. (2008). *Enciclopedia*. Retrieved 22 йил 2011-Marzo from <http://www.iaf.es/enciclopedia/?refer=enciclopedias.com>: <http://www.iaf.es/enciclopedia/?refer=enciclopedias.com>
- Thompson, I. (Octubre de 2008). *Promonegocios.net*. Recuperado el 15 de Marzo de 2011, de Promonegocios.net: <http://www.promonegocios.net/mercadotecnia/definicion-informacion.html>
- Toffler, H., & Toffler, A. (2006). La Revolución de la Riqueza. En Heidi, & A. Toffler, *La Revolución de la Riqueza* (pág. 154). Random House Mondadori.
- Trendmicro. (2010). *TRENDmicro*. Retrieved 2011 йил 22-marzo from [trendmicro.com](http://es.trendmicro.com/imperia/md/content/es/products/data-loss-prevention/datasheet_dlp_es.pdf): http://es.trendmicro.com/imperia/md/content/es/products/data-loss-prevention/datasheet_dlp_es.pdf
- Acevedo, M. (05 de Febrero de 2012). Evite la fuga de la informacion. *Mi empresa*.

- Alegsa. (2009). <http://www.alegsa.com.ar>. Obtenido de ALEGSA: <http://www.alegsa.com.ar/Dic/delito%20informatico.php>
- AENOR . (2003). Seguridad de las Tecnologías de la Información. *AENOR* .
- Business Software Alliance. (2010). *Business Software Alliance (BSA)*. Recuperado el 2011 de Julio de 2011, de <http://www.bsa.org>: <http://www.bsa.org>
- Business Alliance for Secure Commerce. (10 de 09 de 2010). *BASC (Business Alliance for Secure Commerce)*. Obtenido de BASC Costa Rica: <http://www.basc-costarica.com/index.php/descargas>
- Bortnik, S. (01 de Septiembre de 2010). Robo de Información: una tendencia que crece. *ESET Latinoamerica* .
- Borghello, C. (2009). *Seguridad de la Informacion*. Recuperado el 22 de Marzo de 2011, de [segu-info.com.ar](http://www.segu-info.com.ar): <http://www.segu-info.com.ar/logica/seguridadlogica.htm>
- Borghello, C. F. (2009). Amenazas Humanas. (C. F. Borghello, Ed.) *Segu-Info* , 2.
- D'Ambrosio, S. (2009). El concepto de Datos. In R. L. kruse, *Estructura de Datos y Diseño de Programas*.
- Debali, M. D. (2008). Manual de Preparación al Examen CISA. En Mireya Delgado Debali, *Manual de Preparación al Examen CISA* (pág. 276).
- Debali, M. D. (2008). Manual de Preparación al Examen CISA. En M. D. Debali, *Manual de Preparación al Examen CISA* (pág. 357).
- Debali, M. D. (2008). Manual de Preparación al Examen CISA. En M. D. Debali, *Manual de Preparación al Examen CISA* (pág. 95).
- Definición. (2008). *Definicion*. Retrieved 22 йил 2011-Marzo from definicion.de: <http://definicion.de/conocimiento/>

- Diccionario economico financiero. (Septiembre de 2009). *Diccionario de terminos economicos y financieros*. Obtenido de La Caixa: http://portal.lacaixa.es/docs/diccionario/I_es.html
- ESA-security. (Septiembre de 2009). *ESA Security*. Recuperado el 19 de Abril de 2011, de <http://www.esa-security.com>: <http://www.esa-security.com/web/servicios/analisis.htm>
- Ettore. (Octubre de 1995). Managing competitive intelligence. *ManagementReview* .
- Ediciones El pais S.L. (27 de julio de 2007). La FIA no sanciona a McLaren por el caso de espionaje a Ferrari. *El pais* .
- fistierra. (2011). *fistierra.com*. Recuperado el 2 de marzo de 2011, de fistierra: http://www.fistierra.com/recursos_web/no_explor/diccionarios.asp
- FIA. (2007). *Extraordinary Meeting*. Minuta, Paris.
- Galán Quiroz, L. (1996). *Informática y auditoría para las ciencias empresariales*. Madrid, España: UNA3.
- Gómez, J. S. (2002). *Contrainteligencia Empresarial: herramienta gerencial para la toma de decisiones*. Universidad de Madrid, Especialista en Inteligencia., Madrid.
- Idalberto, C. (2006). Introducción a la Teoría General de la Administración. En C. Idalberto, *Introducción a la Teoría General de la Administración* (7 ed., pág. 110). Mc Graw-hill Interamericana.
- INTECO-CERT. (2009). *www.inteco.es*. Recuperado el 25 de Marzo de 2011, de www.inteco.es: <http://www.inteco.es/Seguridad/>
- ingwebsu. (19 de noviembre de 2008). *Wordpress*. Recuperado el 22 de Marzo de 2011, de INGWEBSU.Wordpress.com: <http://ingwebsu.wordpress.com/2008/11/18/53-amenazas-y-vulnerabilidades/>

- Martínez, B. (26 de Noviembre de 2007). *SIGEA*. Recuperado el 9 de Abril de 2011, de <http://www.sigea.es>:
http://www.sigea.es/index.php?option=com_content&task=view&id=108&Itemid=40
- MEHARI. (2010). Los controles, o medidas, de seguridad se agrupan en subservicios, después en servicios y finalmente en dominios de seguridad. *Introducción 7* © CLUSIF 2010 .
- Merriam-Webster. (23 de Agosto de 2012). *Merriam-Webster*. Obtenido de An encyclopedia britanica company: <http://www.merriam-webster.com/dictionary/insider>
- Miller, J. (2002). O Milênio da Inteligência Competitiva. *Porto Alegre: Bookman* .
- Mistretta, M. (11 de Junio de 2009). Websense: "La pérdida de datos no tiene precio". *b:secure* .
- Ministerio de administraciones publicas. (2006). *MAGERIT - Version 2 Methodology for information Systems Risk Analysis and Managment*. Publicacion, Ministerio de administraciones, Ministerio de administraciones publicas, Madrid.
- Plan General Contable. (2007). <http://www.plangeneralcontable.com/>. Recuperado el 4 de julio de 2011, de <http://www.plangeneralcontable.com/>: <http://www.plangeneralcontable.com/>
- Públicas, M. d. (2009). *Sistematización de actividades del ciclo de vida de los proyectos software*. Madrid: Gobierno de España.
- Pacheco, F. (19 de Enero de 2011). Fuga de información: ¿una amenaza pasajera? . *ESET* .
- Panda Security. (Diciembre de 2009). *Panda Security*. Recuperado el 22 de Marzo de 2011, de [pandasecurity.com](http://www.pandasecurity.com):
<http://www.pandasecurity.com/spain/homeusers/media/pressreleases/viewnews?noticia=5714&ver=20&pagina=9&numprod=&entorno=>
- Panda Security. (2011). *Panda Security*. Retrieved 2011 йил 03-Marzo from [Pandasecurity.com](http://www.pandasecurity.com/mexico/):
<http://www.pandasecurity.com/mexico/>

Pechuan, I. G. (1996). *Sistemas de seguridad y tecnologías de la información para la gestión*. Mexico.

ONU. (11 de Octubre de 2005). <http://www.un.org/es/>. (E. I. Ahon, Ed.) Obtenido de <http://www.un.org/es/>:
www.eclac.cl/publicaciones/DesarrolloProductivo/5/LCW25/LCW25.pdf

Rodicio, C. G. (2010). El concepto de percentil. *Gestión de Proyectos*.

Glosario

DAIS: División Académica de Informática y Sistemas.

UJAT: Universidad Juárez Autónoma de Tabasco.

TI: Tecnologías de la información.

MAGERIT: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.

MEHARI: Método de análisis de riesgo armonizado (por sus siglas en francés).

BSA: Buisness Software Alliance.

SGSI: Sistema de gestión de seguridad de la información.

IC: Inteligencia competitiva.

ALE: Annual Loss Exèctamcy (esperanza de pérdida anual).

EAC: Estimated anual cost (Costo anual estimado).

ISO: International Organization for Standarization (Organización Internacional de Estandarización).

Anexos y Apéndices

Informe del Modelo de Análisis para la Prevención de Riesgos en la Seguridad de Información.

Caso: E&B Promoción Empresarial S.A. De C.V.

Villahermosa Tabasco a 14 de noviembre del 2011

E&B Promoción Empresarial S.A. de C.V.

Gerencia de Calidad

A quien corresponda.

Estimados señores me es grato comunicarles que después de concluir el análisis que generosamente me permitieron hacer a su empresa, me permito puntualizar en las siguientes áreas de mejora en las cuales me gustaría poder participar como parte de su equipo en el despliegue y manejo del cambio.

A continuación enumero las propuestas para salvaguardar los activos con riesgos de mayor frecuencia e impacto.

1. Infomercados:

a. Acceso

1. Seguir trabajando con la paquetería actual añadiendo la protección de la documentación.
2. Comunicar oportunamente y con un estándar de envíos en PDF a clientes internos y externos.
3. Programar de manera oportuna la carga y descarga de la información.

b. Integridad

1. Activar y desactivar en tiempo cuentas de usuarios.
2. Limitar accesos.
3. Determinar tiempos de uso de los diferentes sistemas.

c. Robo o extravío

- 1. Instituir penalizaciones en caso de la extracción no autorizada de la información.
 - 2. Crear una política incluyente para el correcto manejo de la información.
 - 3. Reglamentar el uso de los equipos y en caso de pérdida el costo de reembolso o en su defecto la reposición de los mismos.
 - d. Seguridad general
 - 1. Adquisición de un equipo que permita disminuir el impacto de las descargas o apagones eléctricos.
 - 2. Equipos de información (hardware)
 - a. Integridad
 - i. Team Viewer Remote Control Application.
 - b. Relación
 - i. Monitorear de forma remota (TeamViewer).
 - ii. Comunicar , capacitar y dar seguimiento (Skype).
 - c. Robo o extravío
 - i. Almacenar y respaldar (Dropbox).
- Impacto con mayor frecuencia
- i. Xaguar
 - a. Integridad
 - i. Modificar el sistema de tal forma que pueda ligar el control de viáticos con el plan de visitas en PDV y la nómina.
 - ii. Control de asistencia por huella digital.
 - iii. Administrar los accesos al sistema de información tanto para captura como para consulta.
 - b. Seguridad general
 - 1. Modificar el sistema para que genere un respaldo de toda la información semana a semana.
 - c. Relación
 - Administración de personal.
 - Viáticos.

- Nominas.
- Infomercados (interno)
 - a. Integridad.
 - i. Grupos de trabajo para consulta, desarrollo e integración mediante conferencias (Skype).
 - b. Relación
 - i. Hacer el feedback de los procesos ejecutados para el nuevo plan.
 - ii. Trabajo sobre fechas de entrega.
 - iii. Supervisión remota y capacitación no asistida.

Anexo a este documento encontrara 3 propuestas que podrían ser de mucha utilidad para su empresa. Quedo a sus órdenes y una vez más le reitero mi agradecimiento por todo el apoyo brindado a este estudio.

Queda de usted

Ing. José Manuel Torres Hernández.

MODELO DE ANÁLISIS PARA LA PREVENCIÓN DE RIESGOS EN LA SEGURIDAD DE INFORMACIÓN. CASO: E&B PROMOCIÓN EMPRESARIAL S.A. DE C.V.

ORIGINALITY REPORT

17%

SIMILARITY INDEX

PRIMARY SOURCES

1	repositorio.upsin.edu.mx Internet	348 words — 2%
2	www.scribd.com Internet	257 words — 1%
3	docplayer.es Internet	227 words — 1%
4	archivos.ujat.mx Internet	170 words — 1%
5	es.slideshare.net Internet	167 words — 1%
6	seguinfo.wordpress.com Internet	159 words — 1%
7	repositorio.uci.cu Internet	158 words — 1%
8	www.latinoseguridad.com Internet	156 words — 1%
9	pis2.wikispaces.com Internet	85 words — < 1%

10	www.coursehero.com Internet	85 words — < 1 %
11	hdl.handle.net Internet	81 words — < 1 %
12	chelotrip-ti.blogspot.com Internet	79 words — < 1 %
13	prezi.com Internet	77 words — < 1 %
14	luizhiz93.blogspot.com Internet	75 words — < 1 %
15	tedorin.wordpress.com Internet	75 words — < 1 %
16	inf-tek.blogia.com Internet	74 words — < 1 %
17	ddd.uab.cat Internet	67 words — < 1 %
18	repositorio.uesiglo21.edu.ar Internet	66 words — < 1 %
19	delacruzvera.blogspot.com Internet	65 words — < 1 %
20	www.pymesyautonomos.com Internet	57 words — < 1 %
21	www.slideshare.net Internet	55 words — < 1 %

22	elprofedenaturales.wordpress.com Internet	54 words — < 1 %
23	intra.uigv.edu.pe Internet	49 words — < 1 %
24	fdocuments.net Internet	40 words — < 1 %
25	www.clubensayos.com Internet	40 words — < 1 %
26	petalofucsia.blogia.com Internet	39 words — < 1 %
27	nanopdf.com Internet	38 words — < 1 %
28	issuu.com Internet	35 words — < 1 %
29	portal.lacaixa.es Internet	35 words — < 1 %
30	cronicaseguridad.com Internet	34 words — < 1 %
31	documents.mx Internet	33 words — < 1 %
32	es.scribd.com Internet	33 words — < 1 %
33	esa-security.com Internet	32 words — < 1 %

EXCLUDE QUOTES	ON	EXCLUDE SOURCES	OFF
EXCLUDE BIBLIOGRAPHY	ON	EXCLUDE MATCHES	< 30 WORDS