UNIVERSIDAD JUÁREZ AUTÓNOMA DE TABASCO

DIVISIÓN ACADÉMICA DE INFORMÁTICA Y SISTEMAS

PLANEACION EN LA SEGURIDAD DE LA INFORMACIÓN PARA CENTROS DE DATOS EN ORGANIZACIONES DE GOBIERNO

Trabajo recepcional bajo la modalidad de Tesis

Que para obtener el grado de

Maestro en Administración de Tecnologías de la Información

Presenta

Adrián Sadí Gutiérrez Alonso

Asesores

MIS. Isaías Hernández Rivera
MTE. Oscar Alberto González González

Cuerpo(s) Académico(s):

Telecomunicaciones y Redes
Tecnología Instruccional

Líneas de Generación y Aplicación del Conocimiento:

Infraestructura de Software de Redes
Infraestructura de Hardware de Redes

Cunduacán, Tabasco Enero 2012

UNIVERSIDAD JUÁREZ AUTÓNOMA DE TABASCO

DIVISIÓN ACADÉMICA DE INFORMÁTICA Y SISTEMAS

PLANEACION EN LA SEGURIDAD DE LA INFORMACIÓN PARA CENTROS DE DATOS EN ORGANIZACIONES DE GOBIERNO

Trabajo recepcional bajo la modalidad de Tesis

Que para obtener el grado de

Maestro en Administración de Tecnologías de la Información

Presenta

Adrián Sadí Gutiérrez Alonso

Asesores

MIS. Isaías Hernández Rivera

MTE. Oscar Alberto González González

Revisores

MASI. Arturo Corona Ferreira

M. en I.S. Homero Alpuin Jiménez

M. en I.S. José Hernández Torruco

Cunduacán, Tabasco Enero 2012

UNIVERSIDAD JUÁREZ AUTÓNOMA DE TABASCO

"ESTUDIO EN LA DUDA, ACCIÓN EN LA FE"

DIVISIÓN ACADÉMICA DE INFORMÁTICA Y SISTEMAS

Oficio No. 2708/11/DAIS/D
Diciembre 09 de 2011

M.I.S. Isaías Hernández Rivera
Profesor-Investigador
P r e s e n t e

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 **"Planeación en la seguridad de la información para centros de datos en organizaciones de gobierno"**, a realizarse por el Ing. Adrián Sadí Gutiérrez Alonso, para obtener el Grado de Maestro en Administración de Tecnologías de la Información bajo la modalidad de Tesis

Sin otro particular, aprovecho la oportunidad para enviarle un cordial saludo.

Atentamente

M.A. Rubicel Cruz Romero
Director

Universidad Juárez Autónoma de Tabasco
División Académica de Informática y Sistemas

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

Oficio No. 2709/11/DAIS/D
Diciembre 09 de 2011

M.T.E. Oscar Alberto González González
Profesor-Investigador
P r e s e n t e

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 **"Planeación en la seguridad de la información para centros de datos en organizaciones de gobierno"**, a realizarse por el Ing. Adrián Sadí Gutiérrez Alonso, para obtener el Grado de Maestro en Administración de Tecnologías de la Información bajo la modalidad de Tesis

Sin otro particular, aprovecho la oportunidad para enviarle un cordial saludo.

Atentamente

M.A. Rubicel Cruz Romero
Director

Universidad Juárez Autónoma de Tabasco
División Académica de Informática y Sistemas

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

Carta de Autorización

A quien corresponda

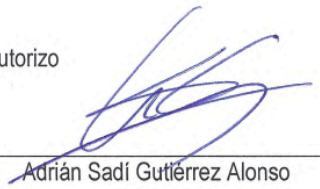
El que suscribe, autoriza por medio del presente escrito a la Universidad Juárez Autónoma de Tabasco para que utilice tanto física como digitalmente la tesis de grado denominada, **"Planeación en la seguridad de la información para centros de datos en organizaciones de gobierno"**, de la cual soy autor 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 más no limita 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 manifiesto, 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 éste documento.

Se firma la presente autorización en la ciudad de Villahermosa, Tabasco a los 16 días del mes de Enero del año 2012.

Autorizo



Adrián Sadí Gutiérrez Alonso

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 "Planeación en la seguridad de la información para centros de datos en organizaciones de gobierno", realizado por el Ing. Adrián Sadí Gutiérrez Alonso, 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.

MIS. Homero Apuin Jiménez
Profesor-Investigador

MASI. Arturo Corona Ferreira
Profesor-Investigador

MIS. José Hernández Torruco
Profesor-Investigador

UNIVERSIDAD JUÁREZ AUTÓNOMA DE TABASCO

"ESTUDIO EN LA DUDA. ACCIÓN EN LA FE"

DIVISIÓN ACADÉMICA DE INFORMÁTICA Y SISTEMAS

Oficio No.0061/12/DAIS/D
Enero 17 de 2012

ING. Adrián Sadi Gutiérrez Alonso
P R E S E N T E

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 **"Planeación en la seguridad de la información para centros de datos en organizaciones de gobierno",** 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

Universidad Juárez Autónoma de Tabasco
División Académica de Informática y Sistemas

M.A. Rubicel Cruz Romero
Director

c.c.p. Lic. Martha Patricia Silva Payró.- Coordinadora de Investigación y Posgrado.
Asesores: M.I.S. Isaías Hernández Rivera; M.T.E. Oscar Alberto González González
Archivo.
Consecutivo.

Dedicatoria

A mi amada esposa Lizbeth por su gran apoyo brindado día con día, por animarme a entrar a la maestría, por aguantar mis desveladas, mis frustraciones y por los sacrificios realizados.

A mi amado hijo Angel Iván por su cariño y apoyo durante todos los sábados en que asistí a clases.

A mis padres y hermanas por estar al pendiente de mí y mi familia en los momentos más importantes.

A mis suegros por todo su apoyo y por estar al pendiente de mi familia.

A mis maestros por todas sus enseñanzas en el aula, por su experiencia y sus sabios consejos.

A mis asesores Oscar e Isaías por guiarme en este camino para conseguir la meta deseada.

Agradecimientos

A la División Académica de Informática y Sistemas le estoy infinitamente agradecido por todas las facilidades que me otorgaron para poder realizar y concluir mis estudios de maestría. A nuestro director muchas gracias.

Le agradezco a la coordinación de investigación y posgrado a cargo de la maestra Martha Patricia Silva Payro por su apoyo, las facilidades brindadas, sus recomendaciones y por haber estado al tanto de cada uno de nosotros los estudiantes de posgrado para todos los tramites que tuvimos que realizar.

A mi alma mater la Universidad Juárez Autónoma de Tabasco por darme la oportunidad de conocer e ingresar a su programa de posgrado.

Gracias a todos mis compañeros de aula por conocerlos y por compartir nuestras experiencias tanto profesionales como laborales, y por haber tenido la oportunidad de intercambiar puntos de vista que enriquecen nuestra vida profesional.

Especial agradecimiento a mis asesores por todo el apoyo y su dedicación que me brindaron para las revisiones de este trabajo de investigación.

Agradezco también a mis revisores que conformaron la comisión revisora y a toda la planta de maestros de la DAIS.

Índice

Índice de ilustraciones

Índice de tablas

Resumen

Las organizaciones de gobierno actualmente están empleando las tecnologías de la información y comunicación para mejorar la calidad de los servicios que proveen a otras organizaciones dentro del mismo gobierno, a proveedores y a los ciudadanos. Modernizar e innovar en los servicios no ha sido una tarea fácil ya que implica la reingeniería de procesos existentes, y el diseño de los nuevos procesos para la implementación de los nuevos sistemas institucionales, la interconexión de la gran red de gobierno, las redes sociales, las transacciones en línea, los portales informativos conllevan a que los riesgos a la seguridad de la información que es almacenada, procesada y transmitida en los centros de datos tengan que ser analizados para evitar que se materialicen las vulnerabilidades y ocasionen daños irreversibles, mediante una adecuada planeación.

El objetivo de esta investigación es planear la seguridad de la información en los centros de datos de las organizaciones de gobierno. Existen muchas formas de ver la planeación de la seguridad, en ocasiones se les llama programas de seguridad, es por ello que este trabajo está apoyado con la norma internacional la ISO 27000 para comprender en qué consiste la planeación de la seguridad de la información, sin llegar a su implementación.

El estudio es de corte cualitativo, se emplea el marco de referencia de evaluación organizacional y para aumentar la validez del estudio se triangula con los marcos de referencia hermenéutica y el etnográfico, se emplea la técnica de entrevista informal y la revisión documental sobre el tema de estudio. Los estudios cualitativos son inductivos porque no buscan generalizar sus resultados, estudian un caso y buscan obtener de él la mayor información. La evaluación organizacional se realizó aplicando técnicas como DOFA y causa-efecto de Hishikawa, en donde se obtienen los ejes de análisis de la investigación, posteriormente se lleva a cabo la relación de los ejes de análisis obtenidos con la norma ISO 27001.

En la norma ISO 27000 el proceso de planeación se centra en la evaluación de los riesgos de seguridad, por ello durante el desarrollo de la metodología se describe el análisis de riesgos desde una perspectiva cualitativa, y se hace uso de las técnicas de obtención de información para la evaluación de corte cualitativo, así como la herramienta OCTAVE para enlistar los activos y las amenazas, los riesgos a la infraestructura y la planeación de la seguridad que como resultado nos plantea la interrelación de los ejes analizados con la información obtenida de las entrevistas y citas de diversos autores que refuerzan los puntos analizados, para el caso estudiado se presentan las recomendaciones de la norma para cada uno de los ejes de análisis y una vez seleccionados los controles, se plantea la planeación de la seguridad en términos de mitigar los riesgos de seguridad.

Se presentan las conclusiones obtenidas de esta investigación y la propuesta para trabajos futuros.

Capítulo I. Introducción

En este capítulo se abordan los antecedentes, el planteamiento del problema, el objetivo general y los específicos para efectuar la planeación de seguridad de la información para centro de datos en organizaciones de gobierno y la metodología empleada para llevar a cabo la investigación.

1.1 Antecedentes

Un tema importante hoy en día de acuerdo a Clempner y Gutiérrez, (2002) es la necesidad de incorporar las tecnologías de información para generar ventaja competitiva en las organizaciones, para las que los riesgos se han incrementado, dado que la administración, consolidación e integración de recursos de TI es una actividad compleja.

Clempner y Gutiérrez (2002) afirman que la TI se desarrolla de una forma reactiva, en respuesta a las necesidades urgentes de negocio lo que produce islas de TI a lo largo y ancho de las áreas funcionales, que no crecen coherentemente hacia una arquitectura integrada de sistemas, tecnología e información.

Es poco el esfuerzo realizado para especificar las estrategias de negocio y construir un modelo de la organización, como precursores en la especificación de los requerimientos de TI. (Clempner & Gutiérrez, 2002)

Aunado a esta complejidad que implica la incorporación de las TI, en la actualidad nos enteramos por las noticias sobre incidentes de seguridad presentes cada vez con más frecuencia. Ejemplos de este tipo de noticias pueden ser la intrusión a páginas web de gobierno o grandes empresas, estafas por ingeniería social a través del correo electrónico, robo de información, falsificación de identidad, falsificación de tarjetas de crédito.

Los principales hallazgos del estudio sobre seguridad empresarial presentado por la empresa Symantec realizado en latino américa en 2010, fueron:

- La seguridad empresarial es la principal preocupación para Tecnologías de la Información.
- Las empresas están sufriendo ataques frecuentemente.
- Los costos de los ataques cibernéticos son altos.
- La seguridad empresarial se está volviendo más difícil.

Según el mismo estudio de 2100 empresas participantes el 100% dijeron haber experimentado pérdidas durante 2009. Las más significativas fueron: robo de propiedad intelectual, inactividad en sus entornos, robo de información de tarjetas de crédito.

A nivel mundial el robo a información de tarjeta de crédito, identificación personal y propiedad intelectual son señaladas en el estudio como las tres consecuencias principales de la pérdida de datos.

El propósito de la protección de la información es preservar los recursos valorados de la organización tales como la información, el hardware y el software. (Peltier, Peltier, & Blackley, 2005)

Todas las organizaciones poseen información o datos, que son críticos o sensibles. (Calder & Watkins, 2008)

Según Alger (2005) los centros de datos son lugares con ambientes especializados que resguardan los equipos y la propiedad intelectual, es decir, lo más valorado de la empresa. Por eso a este lugar lo considera como el cerebro de la empresa.

El negocio a través de su centro de datos percibe el mundo y se comunica a través de las redes de datos y los servicios de correo, se almacena la información y se desarrollan nuevas ideas, todo esto recae en su correcto funcionamiento.

Para Jayaswal (2006) los centros de datos deben contar con dos tipos de seguridad:

1. Seguridad física: mantener alejadas a las personas que no tienen necesidad de estar en él.
2. Seguridad lógica: prevenir el acceso no autorizado a través de la red.

La seguridad física tiene que ver con los dispositivos o medios que monitorean o restringen los accesos de personas al centro de datos. Pueden ser lectoras de control de acceso ubicadas en los puntos de entrada o cámaras que vigilan las rutas y los accesos al centro de datos.

En cuanto a la seguridad lógica, la información más valiosa de las organizaciones se almacena en línea. Es importante prevenir el acceso ilícito a los datos haciendo más difícil a los intrusos, estableciendo diferentes niveles de seguridad.

De acuerdo a Hill (2009) la información es fuente primaria de ventaja competitiva para muchas empresas.

La pérdida física permanente de información clave o la perdida de confidencialidad de información sensible podrían tener un impacto negativo severo en una empresa.

Se considera protección de los datos a la mitigación del riesgo de pérdida o al daño de los datos en la empresa.

Esta pérdida puede adoptar muchas formas, la pérdida física por sí misma sea temporal o permanente, la pérdida de confidencialidad de datos sensibles, la pérdida de disponibilidad de poder usar los datos ocasionado por falta de acceso o una pérdida de respuesta en la cual los datos no pueden ser recuperados para usarse, aún si está técnicamente disponible, dentro de un periodo de tiempo razonable.

Según Vellani (2007) existen tres tipos de contramedidas empleadas para prevenir, mitigar y eliminar el riesgo. Estas son las políticas y procedimientos, la seguridad física y la seguridad del personal.

El manejo de datos sensibles, las atribuciones legales y su autoridad para definir normativas gubernamentales relacionadas con las políticas de seguridad de la información en la protección de los datos que se almacenan o transmiten por las redes de voz y datos de gobierno, hacen a la organización objeto de este estudio, sujeto de protección de identidad. Por ética de los investigadores, para proteger la integridad de la organización objeto de este estudio, se hará referencia a ella como “la organización”

El objetivo de la organización de gobierno bajo estudio es apoyar con consultorías, asesorías, capacitación y normatividad tecnológica y de comunicaciones a los procesos de modernización e innovación, así como de desarrollo organizacional para las entidades y dependencias de la administración pública estatal.

El reglamento interior señala que la organización tiene la atribución de diseñar e implementar las políticas de uso y seguridad de la información.

La red de gobierno está conformada por la interconexión de las redes de voz y datos de todos órganos de gobierno del ejecutivo estatal, si bien en la actualidad a pesar de los esfuerzos realizados no todos los organismos tienen una interconexión directa por medios de comunicación propios para hacer uso de la intranet, muchas dependencias hacen uso de los sistemas gubernamentales a través de internet.

La red de gobierno se creó como una solución para agilizar la comunicación entre dependencias, ya que sólo existían islas de información, algunas de ellas estaban enlazadas pero no compartían comunicación de voz.

Por esta razón se enlazaron 15 dependencias, 9 conmutadores, con alrededor de 3365 usuarios de datos y 863 de voz, permitiendo la comunicación a través de protocolos de voz sobre ip.

Además con la instalación de un anillo de fibra óptica en el edificio de gobierno se enlazaron 6 dependencias, lo cual permite ahorros en el servicio telefónico, acceso a sistemas gubernamentales, optimización del servicio de internet por medio de infraestructura propia convergiendo en un centro de datos, el cual hospeda los servidores de misión crítica de las dependencias con una infraestructura robusta de respaldo y seguridad cuyo principal objetivo es resguardar la información.

La tesis aborda el tema de la seguridad con la finalidad de dar a conocer los aspectos importantes en esta materia, que permitan diseñar y proponer a la organización un plan de seguridad de la información que contribuya a que en el futuro pueda optar por la adopción de un modelo de gestión de la seguridad de la información de acuerdo a normas internacionales.

1.2 Planteamiento del problema

La introducción de nuevos sistemas integrales de gestión gubernamental ha generado un mayor crecimiento de la red gubernamental, conectando más redes de otras dependencias, estos puntos de interconexión pueden ser un riesgo potencial para la seguridad de la información si no cuentan con un adecuado control de los accesos y el monitoreo permanente de los mismos.

Los servicios de atención y contacto con los ciudadanos se han transformado gracias a la incorporación del internet, las redes sociales, el correo electrónico. Más y nuevos servicios se ofrecen al ciudadano empleando kyoskos o accediendo a portales web desde cualquier lugar por internet.

Xuanzi (2006) considera que con la amplia aplicación de grandes y complicadas redes en todos los campos, así como el desarrollo de técnicas de ataque y la diversidad de medidas adoptadas, proteger la información del negocio se ha vuelto un problema importante.

De manera periódica despachos externos realizan auditorías en la organización con la finalidad de revisar cómo se lleva a cabo el proceso en seguridad de la información para algunos sistemas de información críticos.

Al término de estas auditorías son presentadas las recomendaciones que en resumen giran en el entorno de las estrategias de TI, los puntos que son necesarios fortalecer dada la falta de planeación en tecnologías de la información, la falta de una política de seguridad de la información, la ausencia de planeación de la seguridad de la información, y por último la falta de controles de seguridad física en el centro de datos.

Weil (2004) afirma que las medidas de seguridad de la información están incrementándose constantemente en alcance, complejidad e importancia. Así también plantea que existe una necesidad imperante de mantener la seguridad de la información con procesos estandarizados e integrados basados en mejores prácticas, puesto que se ha vuelto riesgoso, costoso e ineficiente para las organizaciones tener la seguridad de su información dependiendo de procesos apresurados y mal planeados.

Según un estudio de la empresa Deloitte publicado en 2009, para el 56% de las empresas financieras encuestadas las restricciones presupuestarias supone el mayor impedimento para garantizar la seguridad de la información vea la Ilustración 1.1.

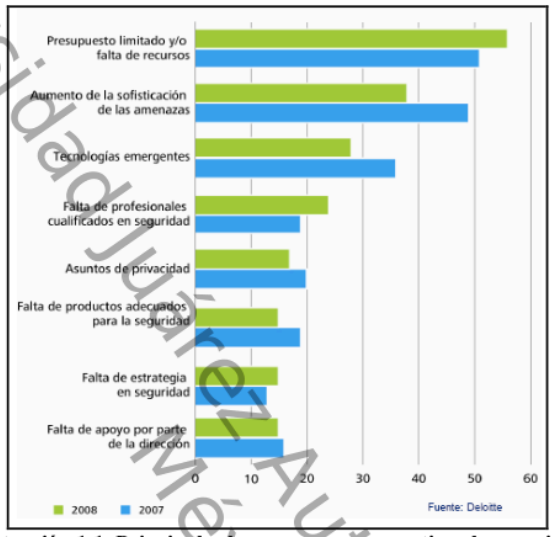


Ilustración 1.1. Principales barreras para garantizar la seguridad
Fuente: Informe anual de seguridad en instituciones financieras (Deloitte,2009)

Otra de las grandes preocupaciones en las entidades según la encuesta realizada por Deloitte es la falta de personal especializado en la materia.

Actualmente no existe en la estructura de la organización un área que se encargue específicamente de la administración de la seguridad de la información, tampoco se efectúa la práctica de administración de riesgos, no se planea la seguridad ante una contingencia de cualquier naturaleza dado que no está establecida la política y los procedimientos de seguridad de la información para la organización.

Expertos aseguran que la seguridad de la información es un problema de personas, otros piensan que es un problema de tecnología, ambos puntos de vista son correctos. Pero antes de que se pueda hacer algo al respecto, la alta dirección debe involucrarse en la seguridad de la información, asignar recursos suficientes y comunicar claramente que la seguridad de la información es realmente importante. (Cresson, 2002)

Por ello surge la afirmación de que la seguridad de la información es un problema de la alta dirección en las organizaciones.

La falta de apego y adopción por parte de las entidades gubernamentales a las normas internacionales sobre la seguridad de la información reflejan un bajo grado de madurez en los procesos relacionados con las TIC's.

Dada esta carencia de planes estratégicos de tecnologías de información, a la poca claridad en la administración pública estatal para el ámbito de las tecnologías de información y comunicaciones, y principalmente que se deja a un lado el enfoque en la seguridad de la información siendo esta información un activo invaluable tanto para la organización como para el Estado. Por lo anterior se planteó la necesidad de diseñar un plan de seguridad de la información que puede ser utilizado por cualquier dependencia que desee saber cómo enfrentar el problema de la seguridad en sus centros de datos.

1.3 Objetivo general

Planear el aseguramiento de la información de la organización con apego a las normas ISO 27001 y 27002 con el fin de controlar y proteger los activos de información de la organización.

1.3.1 Objetivos específicos

- Analizar los procesos que conforman la seguridad de la información de acuerdo a la norma ISO 27000 que permita aplicar herramientas de aseguramiento de la calidad.
- Diagnosticar la situación actual del caso de estudio indicado con respecto a la seguridad de la información aplicando el análisis de riesgo cualitativo.
- Identificar recomendaciones de la norma 27002 aplicables a este caso de estudio, para conocer las guías de implementación propuestas por cada control.

1.4 Justificación

Generalmente en los planes estatales de desarrollo se establecen objetivos y metas que se pretenden llevar a cabo durante la gestión pública, dentro de ellos se encuentran líneas de acción orientadas a fortalecer la infraestructura que permitan la modernización de los servicios de la administración pública.

La incorporación y el uso de las tecnologías de la información es una condición necesaria en el proceso de modernización de la administración pública, mantener actualizadas las herramientas que permiten controlar los procesos, contar con información oportuna y confiable para la toma de decisiones.

A través de las TI se estrechan las relaciones con los ciudadanos, y fortalecen la transparencia en la gestión gubernamental.

La seguridad de la información emplea un sistema de políticas y/o procedimientos para identificar, controlar y proteger de divulgación no autorizada, información que requiere de protección. (Gattiker, 2004)

Las políticas de seguridad informática pueden ser evidencia de los procesos de control de calidad, lo cual puede conferir a un socio la suficiente confianza como para suministrar material confidencial, así como asistir en un proceso de certificación de control de calidad ISO 9000 (Cresson, 2002).

El desarrollo del trabajo se justifica dado que en la organización bajo estudio ya se ha llevado a cabo el proceso de implantación de un sistema de gestión de la calidad bajo la norma ISO 9001, las normas ISO son compatibles entre ellas, por lo que esto conlleva a un beneficio para la organización si en el futuro considera propicio continuar el camino hacia la implantación de un sistema de gestión de la seguridad de la información bajo la norma ISO 27000.

Cabe mencionar que al haber desarrollado el trabajo se contribuye a investigaciones posteriores sobre la seguridad de la información en las organizaciones de cualquier tipo.

Ante la tendencia global de un presupuesto para las tecnologías de la información cada vez más austero, genera una menor inversión en tecnología por lo que el riesgo ante posibles ataques a la red gubernamental crece, por esta razón es importante no solo pensar en términos de seguridad física, seguridad no solo es colocar barreras físicas, hay que poner mayor atención a la seguridad de lo intangible ya que el daño puede ser incalculable.

Por el tamaño que actualmente ha alcanzado la red gubernamental, al número de usuarios que da servicio tanto en el interior como en el exterior, la seguridad de la información cobra mayor importancia, tomando en cuenta que los centros de datos deben ser una prioridad para el logro de los objetivos planteados en el plan estatal de desarrollo.

Al mismo tiempo haber realizado esta investigación permite contar con una propuesta que beneficia no solo a la organización de gobierno bajo estudio, sino también a otras organizaciones que desean aplicar la seguridad de la información para sus centros de datos, contribuyendo al establecimiento de vínculos con la universidad.

Otro aspecto justificante de este trabajo es que permite al investigador aplicar los conocimientos adquiridos durante su formación profesional y laboral, además, de permitirle continuar fortaleciendo su formación como investigador y el desarrollo del proyecto que le permita obtener el grado de maestro en administración de tecnologías de la información.

1.5 Delimitación

1.5.1 Alcances

- El presente estudio se limita a una serie de recomendaciones que identifiquen los controles para la seguridad de la información en el entorno del centro de datos de la organización bajo estudio con base en las normas 27001 y 27002.

- El presente trabajo sólo publica algunos de los resultados del análisis de los datos, otros no se mencionan con el fin de mantener la confidencialidad de la información de la organización.

1.5.2 Limitaciones

- En este trabajo sólo se abordará el estudio del plan de seguridad de la información bajo la perspectiva del análisis de riesgos con el enfoque cualitativo, por tanto no se contempla su implementación.
- No contar con una autorización para recabar información completa de los centros de datos de la organización.
- La confidencialidad de la información puede no permitir presentar datos e información de los activos que pudieran hacer más amplio el análisis de riesgos.

1.6 Metodología a utilizar

Método del griego mehodos y del latín methodos, modo ordenado de decir o hacer con orden unas cosas, modo de obrar o proceder. Muñoz (1998)

25

Método y metodología son dos conceptos diferentes. El método es el procedimiento para lograr objetivos. Metodología es el estudio del método.

La metodología es el estudio analítico y crítico de los métodos de investigación.

1.6.1 Método de investigación

El trabajo de investigación realizado fue cualitativo y exploratorio. Se abordó el estudio de las normas ISO 27001 y 27002 aplicada al caso de los centros procesamiento de datos para la seguridad de la información.

Según Hernández, Fernández y Baptista (2006) los estudios exploratorios tienen como objetivo examinar un tema o problema de investigación poco estudiado o que no ha sido abordado antes. En este sentido, Rodríguez, Gil y García (1999), mencionan que el método cualitativo tiene como objetivo documentar lo que aún no se ha documentado de un fenómeno.

El método cualitativo posee diversos marcos de referencia. Uno de ellos es de la Evaluación Organizacional. Este marco sirvió como referencia para el presente estudio.

Para dar validez al estudio, se trianguló la Evaluación Organizacional con los marcos de referencia Hermenéutico y Etnográfico. La presentación de los datos se realizó en forma de narración y estadística descriptiva.

Las fuentes de información que se emplearon para la recopilación de la información relacionada con el tema de investigación son primarias y secundarias.

El grado de involucramiento del investigador tiene impacto en la riqueza de los datos que obtiene. (Patton, 2002). En este estudio se usó una observación participativa y un involucramiento total del investigador con lo investigado. En este tipo de observación, el investigador colabora con los sujetos que forman parte del grupo objeto de investigación. De acuerdo con Patton, a estas personas se les denomina colaboradores.

Otras técnicas de obtención de datos empleadas en esta investigación fueron la entrevista informal encubierta y la encuesta. Los instrumentos usados fueron el diario y el cuestionario.

Ambas permiten recopilar la información por medio de preguntas realizadas a los colaboradores.

Las preguntas abiertas que guiaron las entrevistas, no fueron una limitante para identificar variables en la investigación. (Anexo B).

1.6.2 Modelo de Calidad PDCA

El sistema de gestión de la seguridad de la información es un proceso sistemático. Uno de los modelos que sirve como guía en su aplicación es el modelo planear-hacer-verificar-actuar (PDCA

por sus siglas en inglés) vea la Tabla 1.1, el cual utiliza los controles de seguridad detallados en la ISO 27002 (Arnason & Willet 2008).

Fase	Descripción
Planear	Define el alcance y la política del SGSI. Identifica y evalúa los riesgos. Selecciona los objetivos de control y controla el tratamiento de los riesgos. Formula un plan de tratamiento de los riesgos. Se redacta una declaratoria de aplicación.
Hacer	Implementa el plan de tratamiento de riesgos. Implementa los controles seleccionados para alcanzar los objetivos de control en términos de administración de riesgos de negocio.
Verificar	Ejecuta los procedimientos de monitoreo. Lleva a cabo las revisiones. Realiza una auditoria interna.
Actuar	Implementa las mejoras del SGSI.

Tabla 1.1 Modelo PDCA

Fuente: Arnason, S. & Willet, K. (2008). Traducción libre del autor.

Para efectos de esta investigación solo se consideró la fase de planeación.

Capítulo II. Marco teórico

En este capítulo se abordan los antecedentes, los conceptos, la normatividad ISO serie 27000 particularmente requerimientos planteados en la 27001 y los controles en la 27002, en lo que respecta a la seguridad de la información de las tecnologías de la información, se presenta información obtenida de encuestas realizadas en México en años anteriores sobre el tema de estudio tanto en la iniciativa privada como en gobierno.

2.1 Marco referencial

Para alcanzar el objetivo de diseñar un plan de seguridad de la información basado en la norma ISO 27000, es necesario efectuar una investigación documental sobre lo que es un sistema de administración para seguridad de la información ya que plantea el proceso para el aseguramiento de la información de cualquier organización que hace uso de las tecnologías de la información y comunicaciones.

En un estudio reciente realizado en 2009 en colaboración la revista Política Digital y Joint Future Systems (JFS) sobre la percepción de la seguridad de la información en México donde participaron 864 personas que pertenecen al sector público, el 59.60% de los encuestados conocen una norma, estándar o regulación que promueve la seguridad de la información en la dependencia a la que pertenece. Cabe mencionar que el objetivo del estudio es conocer la percepción y el grado de conocimiento sobre aspectos de seguridad de la información de servidores públicos que tienen cercanía o relación con el tema. Algunos de los aspectos investigados fueron: conocimiento de lineamientos, percepción en cuanto al manejo de la información en su dependencia y datos aportados por los ciudadanos, percepción de la difusión de la cultura de la seguridad de la información en su dependencia. Esta investigación se enfocó a personal de áreas de tecnologías de información, planeación, procesos, normatividad y se dirigió a los órdenes de gobierno federal, estatal y municipal. (Política Digital, 2009)

Es de observar en los resultados obtenidos por parte de las personas que respondieron afirmativamente a la pregunta, que si conoce una norma o estándar, que tan solo 5.30% pertenecientes al ejecutivo estatal mencionaron conocer el estándar ISO 27000, del ejecutivo federal 13.99% y en el gobierno municipal solo 3.57%. Vea la Ilustración 2.1.

Se percibe que es bajo el porcentaje de directivos que conocen la existencia de estándares, normas y reglas generales para la seguridad de la información, además, se identifica a las áreas de Tecnologías de Información como las principales difusoras de la cultura de la seguridad de la información. Otros resultados obtenidos del estudio indican que la incidencia de conductas de riesgo es alta, existe una nula capacitación formal con respecto al tema, y se tiene la conciencia de que aún hace falta mucho por hacer en la materia y la difusión de la cultura.

	EJEC. ESTATAL	EJEC. FEDERAL	GOB. MUNICIPAL
SI CONOCEN (mencionaron al menos una):	44.59%	58.13%	30.43%

Estándar o norma	% Ejec. Estatal	% Ejec. Federal	% Gob. Municipal
Reglamento / Guía / Políticas internas	85.61%	65.02%	53.57%
LFTAIP	34.85%	27.98%	75.00%
Comentario no válido	26.52%	14.40%	14.29%
COBIT	8.33%	16.46%	3.57%
ISO 27001	10.61%	15.64%	0.00%
ISO 27000	5.30%	13.99%	3.57%
ITIL	12.12%	10.29%	7.14%
ISO / IEC	9.85%	9.05%	7.14%
Lineamientos de protección de datos personales	3.03%	9.88%	14.29%
ISO 27002 / ISO 17799	3.79%	7.41%	3.57%
BS 7799	1.52%	5.76%	0.00%
IFAI	0.00%	4.53%	10.71%

Ilustración 2.1 Estándares, normas y regulaciones
Fuente: Encuesta de la firma Joint Future Systems (2009)

A este respecto Calder & Watkins (2008, p. 6) consideran que en las organizaciones no existen los sistemas de administración para la seguridad de la información o bien son inadecuados. Calder & Watkins observan en las grandes organizaciones que tienden a operar las funciones de seguridad de manera segregada con poca o más bien sin coordinación. Lo que ocasiona una debilidad estructural en la mayoría de las organizaciones, ya que tienen vulnerabilidades

significativas que pueden ser explotadas deliberadamente o que simplemente la conducen al desastre.

Para Calder & Watkins el tema es complejo y trata sobre todo de la confidencialidad, integridad y disponibilidad de los datos.

De ahí se hace indispensable entender que es la seguridad de la información.

Para Caballero (2009) citado por (Vacca, 2009, p. 225) la seguridad de la información "involucra la protección de activos organizacionales de la interrupción en las operaciones del negocio, modificación de datos sensibles, o divulgar información propietaria".

La seguridad no es un problema de Tecnología de la Información, es un problema del negocio ya que abarca a toda la organización, implica proteger la información y los sistemas del acceso no autorizado, así como su uso, difusión, modificación o destrucción. (Vacca, 2009, p. 225)

Un programa de seguridad de la información es un plan para mitigar los riesgos asociados con el procesamiento de la información. (Wylder, 2004, Cap. 1)

De otro estudio realizado por la empresa especializada Ernst & Young durante el 2009 con respecto a la seguridad de la información, en su 11a edición, de las 1400 empresas encuestadas 100 fueron mexicanas, y del total el 31% son de servicios financieros. A pesar de la situación económica reciente a nivel nacional e internacional los presupuestos destinados a la seguridad se redujeron en un 5% y a pesar de esto en México el 38% reporto un incremento. (b:Secure, 2009)

En el mismo estudio se aborda el tema de riesgos asociado a la seguridad, en México el 44% reconoce hacer un análisis de riesgo formal. Cabe señalar que los presupuestos de tecnologías de información van a la baja pero no así los de seguridad, como hallazgos obtenidos destaca en primer lugar la falta de conciencia en la organización inherente a una falta de cultura de la seguridad que aún prevalece en nuestro país, en segundo lugar la escasez del recurso humano capacitado. (b:Secure, 2009)

Para Martínez (2001) los problemas mas relevantes de nuestra actualidad … engloban el tema del riesgo. Así mismo eventos catastróficos ocurridos como (San Juanico, Ixtoc, paros laborales y

otros) han ido obligando a nuestro país a considerar en los planes de desarrollo global el análisis de riesgos y la gestión de la seguridad en muchos aspectos.

En la actualidad para el gobierno federal es uno de los temás en los que más está poniendo su atención, como son la trasparencia y el acceso a la información, así como garantizar la seguridad y privacidad de la misma.

De lo anterior ya podemos percibir que las organizaciones en nuestro país tendrán que dar un salto cuántico en materia de seguridad de la información, que no solo implica a la tecnología y la infraestructura tecnológica, sino también al negocio en sí, y es aquí en donde la organización a través de un sistema de gestión de la seguridad de la información puede añadir valor, un SGSI con un enfoque de procesos y mejora continua alineado a los objetivos que persiga la organización. Y con este ciclo de mejora ser más eficiente y eficaz en los resultados obtenidos.

La Organización para la Cooperación y Desarrollo Económico (OCDE) establece que debido a la creciente interconexión, los sistemas y las redes de información son más vulnerables, ya que están expuestos a un número creciente, así como a una mayor variedad, de amenazas y de vulnerabilidades. Esto hace que surjan nuevos retos que deben abordarse en materia de seguridad, las directrices se aplican para todos los participantes de la nueva sociedad de la información y sugieren la necesidad de tener una mayor conciencia y entendimiento de los aspectos de seguridad, así como de la necesidad de desarrollar una "cultura de seguridad".

De los trabajos realizados en el taller nacional de seguridad de la información en el sector público de México 2009 se obtienen resultados interesantes:

En cuanto a porque es necesario un sistema de gestión de la seguridad de la información:

- Garantizar la integridad, confidencialidad y disponibilidad de la información
- Garantizar la continuidad de la operaciones
- A través del SGSI resguardar la información que es el activo más importante de las organizaciones
- Mitigar los riesgos a que está sometida la información

En cuanto a controles de seguridad física y técnica:

- Falta normatividad para crear estándares mínimos necesarios para el establecimiento de estos controles.
- Es necesario incrementar la difusión de las políticas de seguridad de la información. También hay que concientizar al funcionario acerca del uso de las políticas de seguridad de la información (cultura de seguridad de la información).
- Existen controles muy deficientes.
- No hay regulación para el manejo de información confidencial por parte de terceros.

Que es lo que hace tan importante la seguridad física en la organización, según Erbschloe (2005) puede ser por varias razones, de las cuales la mayoría tiene su base en lo económico.

Erbschloe considera que primeramente es costoso adquirir, instalar e integrar los equipos en la infraestructura de la organización, en segundo lugar, las operaciones de la organización son dependientes de la infraestructura tecnológica, lo que significa que una interrupción en las operaciones se puede convertir en costos innecesarios y en su caso en una potencial pérdida de ingresos.

En tercer lugar comenta que, las leyes en la mayoría de las naciones en donde hay dependencia de las computadoras, requieren la protección de los datos e información propietaria almacenada en sistemas informáticos así que si esta información se ve comprometida existe la posibilidad de sanciones o acciones legales.

2.2 Marco conceptual

De acuerdo a los fundamentos teórico referidos se establecen los siguientes conceptos para una mejor compresión del tema de investigación.

2.2.1 Seguridad de la información

La norma ISO 27001 (2005) define la seguridad de la información como la "preservación de confidencialidad, integridad y disponibilidad de la información; además de otras propiedades

tales como autenticidad, responsabilidad, no repudio y también puede estar involucrada la confiabilidad".

La definición básica de seguridad gira entorno de estos tres elementos:

- Confidencialidad: Se refiere a prevenir el hacer uso y/o revelar sin autorización la información. La privacidad está cercanamente relacionada a este aspecto.
- Integridad: Significa asegurar que la información sea exacta, completa y no ha sido modificada por usuarios o procesos no autorizados.
- Disponibilidad: Se refiere a asegurar que los usuarios tienen acceso oportuno y seguro a su información.

Estos tres elementos son la base, están ligados en una sola idea que es la de protección de la información. (Wylder, 2004)

2.2.2 Riesgo

El riesgo es definido por Martínez (2001) como "lo malo o el evento indeseable, identificar los posibles escenarios y medir los impactos y consecuencias, de que esto ocurra". (p. 22) Lo cual sugiere dos posibles interpretaciones, una subjetiva o cualitativa y la otra objetiva o cuantitativa.

La International Electrotechnical Commission (IEC) citada por Martínez (2001) define el riesgo como "la combinación de frecuencia o probabilidad y las consecuencias de un acontecimiento peligroso específico". (p. 23) También define el análisis de riesgo como "el uso sistemático de la información disponible para identificar peligros y estimar el riesgo para individuos o poblaciones, propiedades o el medio ambiente". (p. 23)

Martinez (2001) menciona que el análisis de riesgo es un proceso de calidad total o mejora continua.

2.2.3 Análisis DOFA

Koontz & Weinrich citado por López y Correa (2007) con respecto a la matriz debilidades-oportunidades y fortalezas-amenazas (DOFA) define que es "Una estructura conceptual para el analisis sistemico que facilita la comparación entre las amenazas y oportunidades externas con las fuerzas y debilidades internas de la organización". (p. 32)

2.2.4 Análisis causa-efecto

López y Correa (2007, p. 36) menciona que el analisis causa-efecto es una técnica que ayuda a organizar y representar diferentes teorías propuestas sobre las causa de un problema. También se le conoce como Ishikawa o espina de pescado. Es utilizado en la fase de diagnostico y solución del problema.

2.2.5 Centro de datos

Un centro de datos es un lugar muy bien ubicado, seguro donde se alojan y salvaguardan los equipos (servidores, almacenamiento, equipo de comunicaciones, bases de datos, cintas), así como la propiedad intelectual y los datos de una organización.

Snevely (2002) define cinco funciones que requieren y denotan a un centro de datos:

1. Proporcionar un lugar sin peligros y suficientemente seguro para alojar los servidores,
2. Almacenamientos y equipos de comunicaciones,
3. Abastecer de la energía necesaria para mantener la operación de los equipos,
4. Proporcionar un ambiente de temperatura controlada dentro de los parámetros que requieren los equipos para funcionar,
5. Prestar los servicios de conectividad a otros dispositivos tanto dentro como hacia afuera del centro de datos.

Un centro de datos consiste en una sala o cuarto equipado con piso falso de tipo anti-estático, con un sistema de climatización de precisión y control ambiental, un suministro regulado y respaldado de energía eléctrica, con una distribución estratégica de los equipos en filas llamadas pasillos fríos o calientes de acuerdo al sistema de enfriamiento de la sala, un sistema de detección y extinción de incendios, por último cuenta con un acceso restringido a base de controles de acceso y una vigilancia con circuito cerrado.

En ocasiones se le relaciona con la palabra de origen alemán Bunker que no es otra cosa que una edificación construida con la finalidad de proteger algo, en las guerras el objetivo de los bunkers es el de proteger a las personas ante los bombardeos de la aviación o la artillería.

2.2.6 Amenaza

Una amenaza se puede definir con un evento que pueda desencadenar un incidente en la organización, ocasionando daños o perdidas sean materiales o no en sus activos. Estos activos son los recursos informáticos o bienes de tecnología que le permiten a la organización funcionar y alcanzar sus objetivos. Las vulnerabilidades son aspectos que influyen negativamente en un activo y que pueden materializar una amenaza. De materializarse una amenaza se tendría que medir la consecuencia o impacto.

2.2.7 Seguridad física

23

La seguridad física de los sistemas informáticos consiste en la aplicación de barreras físicas y procedimientos de control como medidas de prevención y contramedidas contra las amenazas a los recursos y la información confidencial. (Villalón Huerta, 2002)

2.2.8 Sistema de gestión de seguridad de la información

La ISO 27001 define un Sistema de Gestión de Seguridad de la Información (SGSI), como "aquella parte del sistema de gestión, basada en un enfoque de riesgo empresarial, para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información". (Calder, 2009, p.1)

"El sistema de gestion incluye estructura organizacional, políticas, planeación de actividades, responsabilidades, practicas, procedimientos, procesos y recursos". (International Organization for Standardization, 2005)

La misma organización promueve en la norma internacional 27001 un enfoque de procesos. Un proceso es cualquier actividad que utilice recursos y se administre a fin de permitir la transformación de entradas en salidas. La salida de un proceso frecuentemente puede formar la entrada al proceso siguiente.

Enfoque de procesos dentro de una organización es la aplicación de un sistema de procesos conjuntamente con la identificación, interacción y administración de los procesos.

Cuatro son los puntos importantes a resaltar de la norma.

1. La comprensión de los requisitos de seguridad de la información de una organización y la necesidad de establecer políticas y objetivos de seguridad de la información;
2. Implementar y operar controles para manejar los riesgos de seguridad de la información de una organización dentro del contexto de riesgos totales de negocios de la misma;
3. Monitorear y revisar el desempeño y efectividad del SGSI;
4. Mejoramiento continuo basado en la medición de los objetivos.

La norma adopta un modelo de proceso Planear-Hacer-Comprobar-Actuar (PHCA) conocido en los círculos de calidad como ciclo de Deming por ser el autor del mismo.

Planear – Establecer la política, objetivos, procesos y procedimientos del SGSI pertinentes para gestionar el riesgo y mejorar la seguridad de la información, a fin de entregar resultados conforme a las políticas y objetivos generales de la organización.

Hacer – Implementar y operar la política, controles, procesos y procedimientos del SGSI.

Comprobar – Evaluar y, donde corresponda, medir el desempeño del proceso según la política, objetivos y experiencia práctica del SGSI e informar los resultados a la Gerencia para su examen.

Actuar – Tomar medidas correctivas y preventivas, basado en los resultados de la auditoria interna del SGSI y el examen de la gerencia u otra información pertinente, para lograr la mejora continua del SGSI.

Así mismo el modelo PHCA adoptado por la norma internacional ISO 27001 refleja también los lineamientos establecidos por la OECD en 2002.

2.2.9 Política de seguridad de la información

Gómez (2007) define una política de seguridad como "una declaración de intenciones de alto nivel que cubre la seguridad de los sistemas informáticos y que proporciona las bases para definir y delimitar responsabilidades para las diversas actuaciones técnicas y organizativas que se requieran". Con esta definición se entiende que las políticas de seguridad definen aquellos activos que se deben proteger en la organización.

Las políticas de seguridad informática surgen como una herramienta organizacional para concienciar a los colaboradores de la organización sobre la importancia y sensibilidad de la información y servicios críticos que permiten a la Organización crecer y mantenerse competitiva.

Ante esta situación, el proponer o identificar una política de seguridad requiere un alto compromiso con la organización, agudeza técnica para establecer fallas y debilidades, y constancia para renovar y actualizar dicha política en función del dinámico ambiente que rodea las organizaciones modernas.

La seguridad informática debe ser estudiada para que no impida el trabajo de los operadores en lo que les es necesario y que puedan utilizar el sistema informático con toda confianza. Por eso en lo referente a elaborar una política de seguridad, conviene:

- Elaborar reglas y procedimientos para cada servicio de la organización.
- Definir las acciones a emprender y elegir las personas a contactar en caso de detectar una posible intrusión.
- Sensibilizar a los operadores con los problemas ligados con la seguridad de los sistemas informáticos.

Una política de seguridad puede ser prohibitiva, si todo lo que no está expresamente permitido está denegado, o permisiva, si todo lo que no está expresamente prohibido está permitido.

Los derechos de acceso de los operadores deben ser definidos por los responsables jerárquicos y no por los administradores informáticos, los cuales tienen que conseguir que los recursos y derechos de acceso sean coherentes con la política de seguridad definida.

La importancia de conocer el tipo de información que genera cualquier Organización es fundamental para asignarle el nivel de seguridad apropiado, a través de políticas de seguridad que garanticen el menor riesgo de pérdida de información posible.

2.3 Marco normativo

La ISO 27000 es una serie de normas enfocadas a la gestión de la seguridad de la información. El trabajo de investigación realizado considera aspectos importantes de las normas ISO 27001 y 27002 que se enfocan al sistema de gestión de la seguridad de la información y al código de prácticas o mejores prácticas respectivamente en el ámbito de las tecnologías de la información.

En el ámbito internacional existen dos organismos de normalización: la Comisión Electrotécnica Internacional (IEC), responsable de la elaboración de normas internacionales sobre electrotecnia y electrónica, y la Organización Internacional de Normalización (ISO) que cubre el resto de

sectores de actividad. ISO e IEC comparten la responsabilidad de la elaboración de las normas relativas a las tecnologías de la información. AENOR (2010)

Debido a que International Organization for Standardization tendría diferentes acrónimos en diferentes lenguas ("IOS" en Inglés, "OIN" en Francés para Organisation Internationale de Normalisation) los fundadores decidieron darle una abreviatura corta multipropósito, por ello eligieron ISO que proviene de la palabra griega "isos" que significa "igual". Para cualquiera que sea el país o su la lengua la forma corta del nombre de la organización siempre será ISO. ISO (2010)

La ISO se formó en 1946 por 25 países que se reunieron en Londres y decidieron crear una organización internacional con el objeto de facilitar la coordinación y unificación internacional de estándares industriales. ISO (2010)

Una norma o estándar es una especificación que reglamenta procesos y productos para garantizar la interoperabilidad.

Un estándar internacional (o norma internacional) puede ser usado tanto por aplicación directa o a través de la adopción del mismo, modificando el estándar internacional para adaptarlo a las condiciones locales. La adopción de estándares internacionales resulta en la creación de estándares nacionales equivalentes que son substancialmente los mismos en contenido técnico pero que pueden tener diferencias editoriales en apariencia, uso de símbolos, unidades de medidas, substitución del punto y la coma como marcas decimales y diferencias editoriales resultantes de conflictos con la normativa gubernamental y/o las normativas de requerimientos específicos de la industria, causados por un factor fundamental climático, geográficos, tecnológico o infraestructural, o la necesidad de requerimientos de seguridad que una autoridad de estándares locales considere apropiada.

Los estándares internacionales facilitan el comercio y el intercambio de tecnologías.

Corletti (2006) explica que la Organización Internacional de Estándares (ISO) y la Comisión Internacional de Electrotecnia (IEC) conforman un especializado sistema para los estándares

mundiales. Organismos nacionales que son miembros participan en el desarrollo de normas internacionales a través de comités técnicos establecidos por la organización respectiva para tratar con los campos particulares de actividad técnica. Los comités técnicos de ISO e IEC colaboran en los campos de interés mutuo. Otras organizaciones internacionales, gubernamentales y no gubernamentales, en relación con ISO e IEC, también forman parte del trabajo.

En el campo de tecnología de información, ISO e IEC han establecido unir un comité técnico de unión (Join Technical Committe Nº1/JTC 1). Los borradores de estas normas internacionales adoptadas por la unión de este comité técnico son enviados a los organismos de las diferentes naciones para su votación. La publicación, ya como una Norma Internacional, requiere la aprobación de por lo menos el 75% de los organismos nacionales que emiten su voto. Corletti (2006)

El estándar internacional ISO/IEC 17799 fue preparado inicialmente por el instituto de normas británico (como BS 7799) y fue adoptado, bajo la supervisión del grupo de trabajo "tecnologías de la información", del comité técnico de esta unión entre ISO/IEC JTC 1, en paralelo con su aprobación por los organismos nacionales de ISO e IEC.

El estándar ISO/IEC 27001 es el nuevo estándar oficial, su título completo en realidad es: BS 7799-2:2005 (ISO/IEC 27001:2005). También fue preparado por este JTC 1 y en el subcomité SC 27, IT "Security Techniques". Corletti (2006).

La estructura de la norma ISO/IEC 27001:2005 consta de:

1. Alcances
2. Referencias Normativas
3. Términos y Definiciones
4. Sistema de Gestión de Seguridad de la Información
5. Responsabilidad de la Dirección
6. Auditorías Internas del SGSI
7. Revisión del SGSI por la Dirección

8. Mejoramiento del SGSI

Debido a que la investigación se abocará solamente a proponer un plan de seguridad de la información para un centro de datos basado en el estándar, la investigación se centrará en el análisis de riesgo que se ubica en el punto 4 de la norma ISO 27001, consta de los siguientes incisos que son mostrados por la Tabla 2.1.

Ref.	Descripción
4.1	Requisitos Generales
4.2	Establecimiento y Administración del SGSI
4.2.1	Establecimiento del SGSI
4.2.2	Implementar y Operar el SGSI
4.2.3	Monitorear y Revisar el SGSI
4.2.4	Mantener y Mejorar el SGSI
4.3	Requisitos de Documentación
4.3.1	Generalidades
4.3.2	Control de Documentos
4.3.3	Control de Registros

Tabla 2.1 Incisos del punto 4 de la norma ISO 27001
Fuente: Norma ISO 27001:2005

La correspondencia entre el ciclo Planear, Hacer, Verificar y Actuar (Plan, Do, Check, Act) y los incisos mostrados en la Tabla 2.1 se definen en la Tabla 2.2 a continuación.

Inciso	Descripción	Proceso	Etapas del proceso
4.2.1	Establecimiento del SGSI	Planear	• Definir el alcance del SGSI • Definir la política de seguridad de la información • Definir un enfoque sistemático de la evaluación de riesgo. • Efectuar una evaluación de riesgo para identificar, dentro del contexto de la política y alcance del SGSI, los activos de información importantes para la organización y el riesgo para ellos. • luar el riesgo • Identificar y evaluar opciones para el tratamiento de estos riesgos. • Seleccionar, para cada decisión de tratamiento de riesgo, los objetivos de control y los controles a ser implementados. • Preparar una declaración de aplicabilidad (Statement of Applicability – SoA) o de intención de la organización.
4.2.2	Implementación y operación del SGSI	Hacer	• Formular el plan de tratamiento del riesgo y su documentación, incluyendo procesos planeados y procedimientos detallados. • Implementar el plan de tratamiento de riesgo y los controles planeados. • Proporcionar entrenamiento adecuado para el personal afectado, así como programas de concientización. • Administrar operaciones y recursos en línea con el SGSI. • Implementar procedimientos que permitan la detección temprana de, y respuesta a, incidentes de seguridad.
4.2.3	Monitorear y revisar el SGSI	Verificar	• La etapa de verificación tiene, esencialmente, solo un paso (o conjunto de pasos): monitoreo, revisión, pruebas y auditoria. • Monitoreo, revisión, pruebas y auditoria es un proceso en curso que tiene que cubrir a todo el sistema.
4.2.4	Mantener y mejorar el SGSI	Actuar	• Los resultados de las pruebas y las auditorias deben ser revisados por la administración, al igual que el SGSI a la luz del cambiante entorno del riesgo, tecnología u otras circunstancias; mejoras al SGSI deben ser identificadas, documentadas e implementadas. • A partir de entonces, será objeto de revisión en curso, las pruebas y la aplicación de mejora, un proceso conocido como “mejora continua”.

Tabla 2.2 Correspondencia entre los incisos del punto 4 de la norma ISO 27001 y el proceso PDCA

En conclusión en este capítulo se da una referencia a la investigación con respecto a otros estudios ubicando su contexto, se describen algunos conceptos de aplicación importante para conocer los temas abordados en el trabajo de investigación y se explica cómo está conformada la norma ISO 27001 y 27002 en un enfoque de procesos y las clausulas importantes.

Capítulo III. Aplicación de la metodología y desarrollo

Se define la metodología como "el proceso general de planificación previo al estudio de un fenómeno, ya sea para describir, explicar o transformar la realidad". (Sánchez, 2001, p. 138)

En este capítulo se describe la aplicación de la metodología, tanto para la recopilación de la información como para el desarrollo del trabajo investigación abordando el caso de estudio propuesto.

3.1 Enfoque Cualitativo

Esta investigación es de corte cualitativo, bajo el marco de referencia de Evaluación Organizacional. Para aumentar la validez del estudio, se trianguló con los marcos de referencia Hermenéutico y Etnográfico con un enfoque de cultura organizacional.

La investigación cualitativa para Vasilachis (2006) abarca el estudio, uso y recolección de una variedad de materiales empíricos, estudio de casos, experiencia personal, entrevista, textos observacionales, que describen los momentos habituales y problemáticos y los significados en la vida de los individuos.

De acuerdo a Patton (2002) los estudios cualitativos son de tipo inductivo y no buscan generalizar sus resultados, más bien estudian un caso y obtienen información acerca de él. Los estudios cualitativos tratan primordialmente con la subjetividad, aunque pueden usar técnicas estadísticas para aportar mayor validez a sus resultados.

3.1.1 Metodología de la investigación

Se usó un muestreo cualitativo el cual Patton (2002) define como la menor cantidad de sujetos que proporcionan la mayor cantidad de información rica para el estudio.

La forma de presentación de los resultados fue mediante narración apoyada con gráficos estadísticos.

Se usaron como modelos de análisis la matriz DOFA, diagramas de causa-efecto (Hishikawa) para la identificación de los orígenes del problema y el análisis cualitativo básico de riesgos.

El enfoque cualitativo valora el uso de diversos métodos y técnicas para la obtención de datos con la finalidad de aportar mayor validez al estudio. En el caso de estudio se usaron técnicas de estadística descriptiva e interpretación de los resultados. La primera corresponde a elementos objetivos del estudio y la segunda a la parte subjetiva.

También se realizó una investigación de tipo exploratoria que permitió adentrarse en un tema de estudio pocas veces abordado como la importancia que tiene la seguridad de la información, para lo cual fue necesario la revisión bibliográfica de temas como las normas ISO 27001, ISO 27002, seguridad de la información, seguridad física y lógica, centros de procesamiento de datos, gestión de la seguridad de la información, modelado de procesos, y otros relacionados con el problema planteado para el caso de estudio.

Se validaron los cuestionarios con el auxilio de investigadores expertos en la aplicación y validación de instrumentos para recopilación de información.

Por ética de los investigadores, los nombres de los colaboradores en la investigación, se cambiaron para proteger su identidad.

3.1.2 Estimación de tiempos y costos

Los tiempos y costos derivados de esta investigación se presentan en el Anexo B.

3.2 Desarrollo de la metodología

3.2.1 Evaluación Organizacional

De acuerdo con Patton (2002), existen dos tipos de evaluación organizacional: La sumativa y la formativa.

Las evaluaciones sumativas tienen el propósito de realizar un juicio sobre la efectividad total de un programa, sus políticas o productos, con el fin de decidir si el producto evaluado (evaluand) es efectivo y en consecuencia, si la organización debe seguir aplicando los mismos procesos. (Patton, 2002).

Los datos cualitativos en las evaluaciones sumativas proporcionan profundidad y detalle a los datos obtenidos por técnicas cuantitativas, integran la información obtenida en casos de estudio, en el examen particular de los resultados y en aspectos o aplicaciones de la calidad. (Patton, 2002).

3.2.1.1 Debilidades, Oportunidades, Fortalezas y Amenazas.

Para analizar el contexto organizacional, se usó la técnica DOFA que consiste en la obtención de las estrategias a partir de la identificación de debilidad, oportunidades, fortalezas y amenazas relacionadas con el área de estudio.

Se realizaron entrevistas informales con el propósito de obtener la percepción del personal involucrado con la operación del centro de datos, acerca de la situación actual imperante en cuanto a la seguridad de la información.

Esta percepción se representa empleando un diagrama DOFA (Ilustración 3.1), en él se representan las debilidades, oportunidades, fortalezas y amenazas.

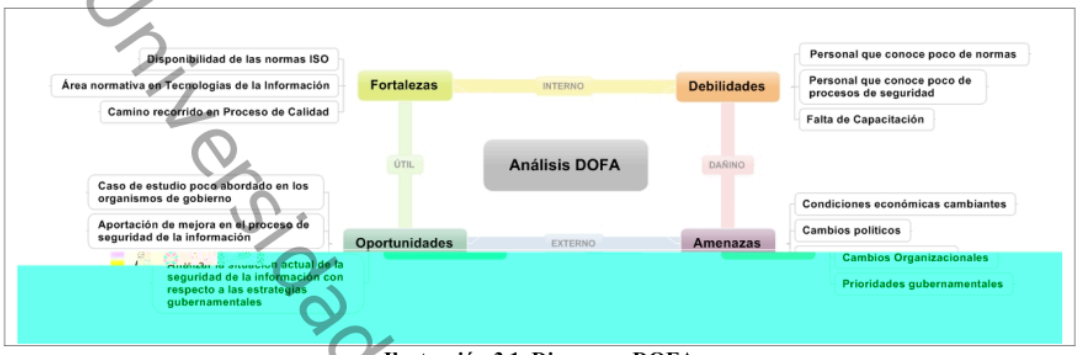


Ilustración 3.1. Diagrama DOFA

La mayor fortaleza del área de tecnologías de la información, es su área normativa. Desde hace dos años se realiza el esfuerzo por establecer un sistema de gestión de la calidad. Ya se han dado pasos para la implantación de la norma ISO 9001.

Jorge, uno de los miembros del staff, refiriéndose a esta fortaleza, mencionó:
"Se modeló el proceso de control de calidad para las áreas de TI, que incluyen desarrollo, soporte e infraestructura. Nosotros formulamos el objetivo, la misión, la visión y buscamos la calidad en nuestros servicios".

Las oportunidades en entidades gubernamentales, son en ocasiones información reservada y sensible tanto para la organización como para sus clientes sean internos o externos, por lo tanto por ética del investigador no se publican en su totalidad a un que se describen brevemente.

Las debilidades están marcadas por la falta de objetivos estratégicos en el PLED dirigidos hacia el tema de la seguridad de la información, el desconocimiento del personal acerca del tema de seguridad de información, falta de procesos documentados, falta de capacitación al personal y desconocimiento de las mejores prácticas en seguridad de la información.

Las amenazas detectadas son:

- las condiciones económicas globales. Estas obligan a redefinir las estratégicas de gobierno ocasionando planes de austeridad y recorte de presupuesto, principalmente los de tecnologías de la información.

- La rotación en los miembros del staff organizacional. Cambian las políticas, y no existe continuidad en los planes de la organización.
- los despidos masivos que afectan a personal clave para la operación.
- Empleados inconformes que pueden ocasionar severos daños a la información o la infraestructura al ser despedidos.
- Desastres naturales que causan afectaciones y generan cambios en las prioridades del gobierno.

La implantación de la norma ISO 27001, es una estrategia que podría agregar valor a la organización aprovechando las oportunidades, reduciendo las amenazas y ayudando a convertir en fortalezas las debilidades de seguridad de la información.

3.2.1.2 Técnica causa – efecto de Ishikawa

Con el fin de diagnosticar y dar solución al problema de la seguridad de la información en la organización, se aplicó la técnica causa efecto de Ishikawa.

Se usaron datos obtenidos en las entrevistas informales con el personal, en la observación directa realizada en el centro de datos de la organización y en análisis de los inventarios. La Ilustración 3.2 muestra las posibles causas raíz y su efecto en la seguridad de la información.

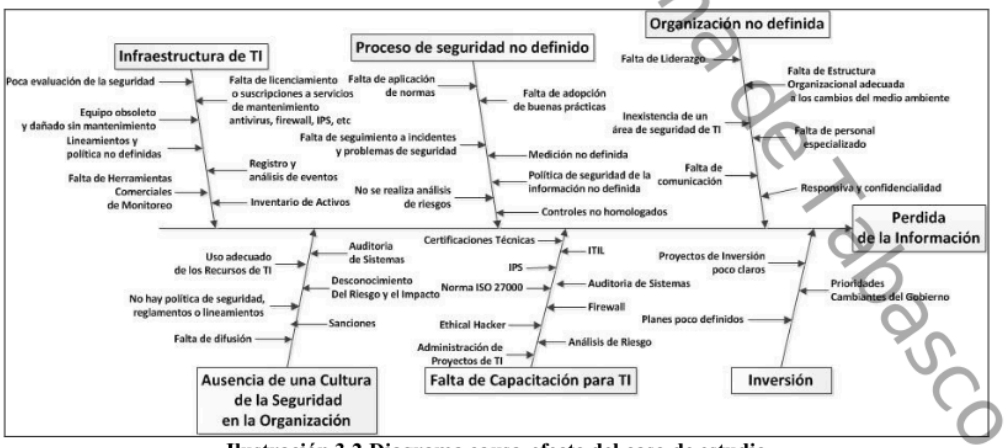


Ilustración 3.2 Diagrama causa-efecto del caso de estudio

El caso de estudio está orientado a la infraestructura tecnológica por ser el centro de datos un lugar físico donde se albergan los equipos de procesamiento, comunicación, ambiente y almacenamiento, lo cual tiene que ver con la infraestructura sin dejar de ser importantes todas las demás.

La espina de infraestructura de tecnologías de la información se obtuvo con base en la observación realizada al centro de datos de la organización. Se pudo observar:

- Ausencia de una bitácora de accesos y de eventos de seguridad
- Distribución inadecuada de los espacios físicos al interior del centro de datos.
- Insuficientes herramientas de monitoreo y control: ambientales, de seguridad física y lógica.
- Carencia de un sistema contra incendio para la detección, la alarma y la extinción.
- Escasos lineamientos y procedimientos para la operación del centro de datos.
- Falta de renovación de equipos de procesamiento y comunicaciones.
- Falta de planeación y ejecución de los mantenimientos preventivo y correctivo a los equipos de procesamiento, almacenamiento, seguridad, comunicaciones, así como renovación de licenciamientos y servicios para el centro de datos.
- se cuenta con un inventario de activos de información inicial pero se carece de un procedimiento y el seguimiento del mismo. La información en el inventario permanece sin movimiento aunque los equipos se encuentran físicamente en otras áreas.

Una vez que se obtuvieron los requerimientos de la organización para la seguridad de la información del centro de datos, se identificaron los activos de información. Se define como activo, todo aquello que tenga valor para la organización.

Aguilera (2010) menciona los activos que se deben identificar para establecer el resguardo y la responsabilidad que tiene el personal encargado de la operación del centro de datos, así como el uso adecuado de los mismos.

- Datos en medios electrónicos.

- Software: sistemas operativos, sistemas de información, aplicaciones comerciales.
- Hardware: servidores, estaciones de trabajo, periféricos.
- Redes: routers, switches, seguridad perimetral Firewall y Proxy, IPS/IDS, PBX, Red inalámbrica; enlaces terrestres y aéreos de microonda y satelital; cableado estructurado y distribución dentro del centro de datos y monitoreo de las comunicaciones.
- Instalaciones.
    - seguridad física: control de acceso, video vigilancia, sistema contra incendios para detección y extinción, alarmas de seguridad
    - sistema de energía ininterrumpida y planta de emergencia
    - ubicación y condiciones: piso falso y plafón, iluminación adecuada, distribución de equipos dentro del centro de datos indicadores y referencias,
    - HVAC (equipo de aire acondicionado de precisión por sus siglas en inglés),
    - instalaciones eléctricas: tableros, distribución de contactos a través de boas, tierra física para protección a equipos electrónicos y protección humana.
- Personal: roles, responsabilidades y funciones.
- Servicios: internet, directorio activo, espacio lógico para almacenamiento y respaldos.

3.2.2 Relaciones entre la norma ISO 27002 y la Evaluación Organizacional

La norma ISO 27000 hace recomendaciones que pueden ayudar a convertir las debilidades en oportunidades y reducir las amenazas, así como los efectos producidos por la causa raíz del problema.

La relación entre la Evaluación Organizacional realizada con base en el análisis DOFA, la técnica de Ishikawa y las recomendaciones de la norma ISO 27002, se muestran en la Tabla 3.1.

Controles de la norma ISO 27002	Evaluación Organizacional	
5. Responsabilidad de la dirección. 5.2. Administración de recursos. (Gestión de recursos suficientes)	Condiciones Económicas globales	Inversión
5. Responsabilidad de la dirección.	Rotación en el staff	Organización no definida
5. Responsabilidad de la dirección.	Despidos masivos	Organización no definida
5. Responsabilidad de la dirección. 5.2.2 Entrenamiento, concientización y competencia	Empleados inconformes	Organización no definida, Falta de capacitación para TI
Objetivos de Control y Controles.	Desastres naturales	Infraestructura de TI
Principios de la OECD (concientización) 5.2.2 Entrenamiento, concientización y competencia	Objetivos de seguridad en la planeación	Ausencia de una cultura de la seguridad en la organización, proceso de seguridad no definido
Principios de la OECD (concientización) 5.2.2 Entrenamiento, concientización y competencia	Desconocimiento del tema	Ausencia de una cultura de la seguridad en la organización, falta de capacitación para TI.
4.3.2 Control de documentos	Falta de documentación	Proceso de seguridad no definido
5.2.2 Entrenamiento, concientización y competencia	Falta de capacitación	Falta de capacitación para TI
Principios de la OECD (concientización) 5.2.2 Entrenamiento, concientización y competencia	Desconocimiento de las mejores prácticas	Ausencia de una cultura de la seguridad de la organización

Tabla 3.1 Relación entre la Evaluación Organizacional y las recomendaciones de la norma ISO 27002.

Del cruce realizado entre los datos obtenidos del análisis de causa y efecto se identifica información que puede ser relacionada y agrupada, tal es el caso de cultura organizacional que integra la capacitación del personal y una organización no definida, además de una ausencia de una cultura de la seguridad.

Entonces se observan cuatro líneas de análisis que serían:

- Económica
- Cultura de la seguridad en la organización
- Infraestructura
- Proceso

3.2.3 Modelo PDCA

El modelo PDCA se ha usado en la industria manufacturera por más de 50 años. Es un ciclo de actividades diseñadas para dirigir la mejora continua. Arnason & Willet (2008), mencionan que, aunque su autor es Walter Shewhart, lo popularizó Edward Deming al difundir los Cuatro Pasos para la Mejora Continua. El modelo PDCA se usa para implementar un SGSI basado en la norma ISO 27001.

La aplicación del ciclo PDCA a un enfoque de proceso implica que se necesitan las entradas y salidas del proceso. Un SGSI toma como entradas los requerimientos y expectativas en seguridad de la información de las partes interesadas, y a través de las acciones necesarias y procesos, produce las salidas de seguridad de la información que cumplen con los requerimientos y expectativas (Ilustración 3.3).

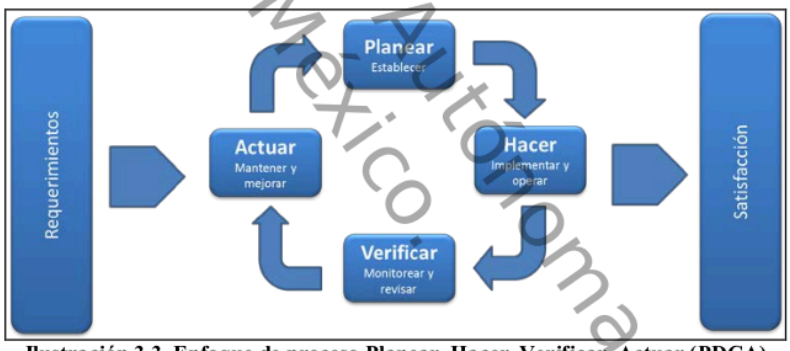


Ilustración 3.3. Enfoque de proceso Planear, Hacer, Verificar, Actuar (PDCA)
Fuente: Tomado y adaptado de International Organization for Standardization. (2010)

El presente proyecto se limita a la fase de planeación.

Fase de planeación

En esta fase: a. se define el alcance del SGSI, b. se define la política del SGSI, c. se identifican y evalúan los riesgos, d. se seleccionan los objetivos de control y controla el tratamiento de los riesgos, e. se formula un plan de tratamiento de los riesgos y f. se redacta una declaratoria de aplicación.

a. Definir alcance del SGSI en función de características del negocio, organización, localización, activos y tecnología, definir el alcance y los límites del SGSI. El SGSI no tiene por qué abarcar toda la organización; de hecho, es recomendable empezar por un alcance limitado.

b. Definir política de seguridad que incluya el marco general y los objetivos de seguridad de la información de la organización, tengan en cuenta los requisitos de negocio, legales y contractuales en cuanto a seguridad, esté alineada con la gestión de riesgo general, establezca criterios de evaluación de riesgo y sea aprobada por la dirección. La política de seguridad es un documento muy general, una especie de declaración de intenciones de la dirección, por lo que no pasará de dos o tres páginas.

c. Definir el enfoque de evaluación de riesgos, definir una metodología de evaluación de riesgos apropiada para el SGSI y las necesidades de la organización, desarrollar criterios de aceptación de riesgos y determinar el nivel de riesgo aceptable. Existen muchas metodologías de evaluación de riesgos aceptadas internacionalmente; la organización puede optar por una de ellas, hacer una combinación de varias o crear la suya propia. ISO 27001 no impone ninguna ni da indicaciones adicionales sobre cómo definirla. El riesgo nunca es totalmente eliminable ni sería rentable hacerlo, por lo que es necesario definir una estrategia de aceptación de riesgo.

- Inventario de activos, todos aquellos activos de información que tienen algún valor para la organización y que quedan dentro del alcance del SGSI.
- Identificar amenazas y vulnerabilidades, todas las que afectan a los activos del inventario.
- Identificar los impactos, los que podría suponer una pérdida de la confidencialidad, la integridad o la disponibilidad de cada uno de los activos.
- Análisis y evaluación de los riesgos, evaluar el daño resultante de un fallo de seguridad (es decir, que una amenaza explote una vulnerabilidad) y la probabilidad de ocurrencia del fallo; estimar el nivel de riesgo resultante y determinar si el riesgo es aceptable (en función de los niveles definidos previamente) o requiere tratamiento.

- Identificar y evaluar opciones para el tratamiento del riesgo, el riesgo puede reducirse (mitigado mediante controles), eliminarse (eliminando el activo), aceptarse (de forma consciente) o transferirse (con un seguro o un contrato de outsourcing).

d. Selección de controles, seleccionar controles para el tratamiento el riesgo en función de la evaluación anterior. Utilizar para ello los controles del Anexo A de ISO 27001 (teniendo en cuenta que las exclusiones habrán de ser justificadas) y otros controles adicionales si se consideran necesarios.

e. Aprobación por parte de la dirección del riesgo residual y autorización de implantar el SGSI, hay que recordar que los riesgos de seguridad de la información son riesgos de negocio y sólo la dirección puede tomar decisiones sobre su aceptación o tratamiento. El riesgo residual es el que queda, aún después de haber aplicado controles (el "riesgo cero" no existe prácticamente en ningún caso).

f. Confeccionar una declaración de aplicabilidad, llamada SOA (Statement of Applicability) es una lista de todos los controles seleccionados y la razón de su selección, los controles actualmente implementados y la justificación de cualquier control del Anexo A excluido. Es, en definitiva, un resumen de las decisiones tomadas en cuanto al tratamiento del riesgo.

3.2.4 Análisis de riesgo

Según Landoll (2011) además de las responsabilidades que implican el rol del administrador de la seguridad de la información en una organización, y que en muchas de las organizaciones varían de acuerdo a su tamaño y su capacidad de inversión, los administradores de seguridad necesitan poder justificar sus proyectos futuros y defender sus decisiones.

Para identificar y priorizar las iniciativas de seguridad a ser presupuestadas en la organización existen algunos enfoques impulsores de iniciativas de seguridad como son:

La auditoría como un impulsor de iniciativas de seguridad en la organización denotan que esta no cuenta con una clara estrategia de seguridad, sin duda los resultados y recomendaciones de una auditoria son importantes para la seguridad de la información, pero su naturaleza es solo la de revisión de lo que se ha hecho de acuerdo a políticas y procedimientos establecidos.

Basada en tecnología. Es claro que siempre existirán en el mercado productos que le permitan a la organización establecer las medidas de protección para sus activos. Landoll considera que una estrategia de seguridad que recae demasiado en la tecnología va a encontrar una ausencia de medidas de protección en las áreas administrativas y físicas.

Cumplimiento con normas en seguridad de la información y requerimientos de la industria. Según Landoll pareciera que es el lugar natural de inicio para crear una estrategia de seguridad para la organización. Una organización necesita dirigirse a los requerimientos en la misión tanto de los clientes como del negocio. El cumplimiento con las normas no proporciona una adecuada guía para la implementación.

Aunque estas aproximaciones ofrecen ciertos beneficios, una estrategia de seguridad más completa puede ser creada en base a un análisis de los riesgos de seguridad. Es el riesgo a los activos de la organización el que necesita ser señalado y la mejor manera es primero medirlo. Según Landoll no siempre la evaluación del riesgo de seguridad es un impulsor para crear una estrategia de seguridad.

La evaluación del riesgo de seguridad está conformada por varias fases que van desde la definición del proyecto, la preparación del proyecto, la obtención de la información administrativa, técnica y física, el análisis del riesgo, la mitigación del riesgo y las recomendaciones.

El Análisis de riesgo es la revisión de los datos obtenidos, para determinar el valor de los activos, criticidad de los sistemas, amenazas probables, y existencia de vulnerabilidades. El analista debe calcular el riesgo por par amenaza/vulnerabilidad para la organización. El cálculo y presentación de estos riesgos puede variar dependiendo del método empleado.

Los elementos que conforman el análisis de riesgo son:

Activos. Son elementos que se consideran de valor para la organización. Primero la enumeración de los activos ayuda a dar alcance a la evaluación de riesgos de seguridad. Segundo ayuda a determinar las contramedidas necesarias, una contramedida es simplemente un control (actividad, técnica, o tecnología) que reduce la posible pérdida para los activos de una organización.

Amenazas y agentes. Una amenaza es un evento con un indeseado impacto, un agente es la entidad que puede causar que ocurra una amenaza. Ambas están interrelacionadas y permiten determinar el alcance de las vulnerabilidades del sistema que está siendo evaluado. Algunos ejemplos de agentes pueden ser: la naturaleza, los empleados, los hackers, espías industriales. Ejemplos de amenazas: Errores y omisiones, fraude y robo, sabotaje, pérdida de soporte físico e infraestructura, código malicioso, revelar información.

Vulnerabilidades. Es un defecto o descuido en un control existente que puede posiblemente permitir que un agente lo explote para obtener acceso no autorizado a activos organizacionales.

Riesgo de seguridad. Es la perdida potencial a un activo de la organización que es probable que ocurra si una amenaza puede explotar una vulnerabilidad. El riesgo de seguridad (y el riesgo residual) es un elemento importante en la evaluación de riesgo de seguridad de la información porque es la culminación de todas las demás evaluaciones, cálculos y análisis.

Hay muchas formas de presentar el riesgo de seguridad pero todas pueden ser descritas como cuantitativas o cualitativas.

La propuesta **cuantitativa** recae en formulas específicas y cálculos para determinar el valor del riesgo de seguridad. Tiene la ventaja de ser objetivo y expresarse en términos monetarios, sin embargo los cálculos pueden ser complejos, los valores exactos de las variables en las formulas pueden ser difíciles de obtener.

La propuesta **cualitativa** recae en medidas subjetivas de valuación de activos, amenazas, vulnerabilidades y el riesgo de seguridad. Tiene las ventajas de ser fácil de entender y en algunos

casos proporciona una adecuada indicación de los riesgos de seguridad de la organización. Al ser una medición subjetiva también puede no ser confiable para algunos administradores.

Los mismos elementos se requieren para determinar el riesgo de seguridad, sean valor del activo, frecuencia de la amenaza, impacto, efectividad de la salvaguarda, pero ahora son medidos en términos subjetivos tales como “Alto” o “No probable”.

En ocasiones las variables cualitativas son expresadas con números, pero no deben ser tratados de la misma manera que los números en un análisis cuantitativo. Cuando el método cualitativo de análisis utiliza números como valores de variables de riesgo de seguridad, estos números son considerados ordinales. Los números ordinales tienen un orden significativo (ej. Alto > Medio > Bajo) pero no hay una métrica para determinar la distancia entre categorías.

Estos números o etiquetas son ordinales y los valores no pueden ser calculados (ej. multiplicados, sumados) para producir resultados de la evaluación.

Las variables de la ecuación del riesgo de seguridad cualitativo no son expresadas en términos de valores monetarios, como una ordenada categoría de pérdida monetaria sea “Crítica”, “Alta”, “Media”, y “Baja”. Las fórmulas para determinar cualitativamente resultados de la evaluación del riesgo de seguridad son simplemente tablas, gráficas, o listas de consulta. (Landoll, 2011)

Para la recopilación de la información necesaria para la evaluación de los riesgos de seguridad cualitativo se recomienda el método RIIOT por sus siglas en inglés que está formado por 5 diferentes enfoques para obtención de datos que pueden ser aplicados en áreas administrativas, físicas y técnicas (Landoll, 2011).

1. **Revisión de documentos.** Revisión en busca de reglas, configuraciones, diagramas, arquitecturas y otros elementos de los controles de seguridad. Así como todos los documentos relevantes disponibles pueden ser revisados, estos incluyen políticas, procedimientos, diagramas de red, distribución de sitio, calendario de respaldos y presentaciones de entrenamiento en seguridad.

2. **Entrevista con personal clave.** Entrevista para determinar sus habilidades para efectuar sus obligaciones (como se declara en las políticas), su ejecución de responsabilidades no declaradas en las políticas, y observaciones o preocupaciones que tienen con los controles actuales de seguridad.
3. **Inspección de controles de seguridad.** Inspección de específicos controles de seguridad implementados tales como control de visitas, archivos de configuración, detectores de humo, y el manejo de incidentes. Estos controles pueden ser inspeccionados con respecto a estándares de la industria, con una específica lista de comprobación (checklist) de vulnerabilidades comunes o mediante el empleo de la experiencia y el criterio.
4. **Observar el comportamiento del personal.** Observar el comportamiento de usuarios, visitantes, el equipo de seguridad y otros durante el transcurso de la evaluación. Estas observaciones pueden proporcionar una aguda comprensión de la efectividad de los controles de seguridad en su sitio.
5. **Probar controles de seguridad.** Probar controles específicos de seguridad tales como firewalls, servidores, alarma de apertura de puertas, sensores de movimiento. Casi todos los métodos de evaluación de riesgos de seguridad actualmente cuentan con este enfoque. Probar involucre el empleo de scanners de vulnerabilidades para controles de seguridad lógica, pruebas de penetración.

En este trabajo de investigación se opta por el método de análisis de riesgo cualitativo primero por ser más sencillo y claro, además de estar en concordancia con el tipo de investigación que se está realizando.

Al realizar un análisis de riesgo cualitativo podemos seleccionar de entre varias metodologías, la de OCTAVE ("The Operationally Critical Threat, Asset, and Vulnerability Evaluation") que es una metodología de evaluación de riesgos de seguridad que fue desarrollada en el Instituto de Ingeniería de Software en la Universidad Carnegie Mellon.

Esta metodología proporciona un proceso completo con lineamientos, listas de comprobación, tiempos estimados, y descripción de las tres fases que conforman el proceso de evaluación de riegos de seguridad, que incluyen:

1. amenazas y activos.
2. Identificación de vulnerabilidades de infraestructura
3. Desarrollo del plan de seguridad

La Tabla 3.2 muestra un comparativo entre algunas metodologías de análisis de riesgo existentes y resume sus fases, los requerimientos y su aplicación.

Metodología	Tipo	Fases	Recursos requeridos	Aplicación
FAA SRM (Federal Aviation Administration) (Security Risk Management)	Cualitativo	• Identificación de Activo • Determinar criticidad del activo • Asignación de criticidad • Identificación de la amenaza • Identificación de contramedidas existentes • asignación de vulnerabilidad del activo • determinación del nivel de riesgo • Toma de decisión • Determinación de la reducción del riesgo • Análisis costo beneficio	• Administradores de programa • Administradores de instalaciones • líderes de equipo de producto integrado • representantes de seguridad	Requerido para Proyectos FAA Método de propósito general
OCTAVE (Carnegie Mellon University)	Cualitativo	• Perfilar amenazas y activos • Identificar vulnerabilidades de infraestructura • Desarrollar estrategia de seguridad y plan	Internos, no expertos	Grandes organizaciones con la habilidad de ejecutar sus propias herramientas.
CRAMM (UK Government)	Herramienta Comercial Cualitativa	• Identificación de activos • Evaluación de amenaza y vulnerabilidad • Recomendación de contramedidas	Practicantes calificados y experimentados	Ha demostrado cumplimiento con BS 7799
NSA IAM (National Security Agency) (Infosec Assessment Methodology)	Cualitativo	• Pre evaluación • Visita en sitio • Post evaluación	Proveedores entrenados IAM	Agencias gubernamentales e infraestructura crítica

Tabla 3.2 Comparativo de Metodologías de evaluación de riesgos de seguridad
Fuente: Tomado y adaptado de Landoll (2011)

En este estudio se ha buscado mantener la confidencialidad de la información de la organización, por esta razón los datos presentados en este análisis tendrán un nombre hipotético para no afectar la sensibilidad de la información proporcionada para llevar a cabo el análisis de riesgo cualitativo, además no se presenta un listado de los activos de información solo se menciona si se trata de un servidor o sistema crítico.

Para realizar el análisis de riesgos de seguridad nos apoyaremos en el método de presentación de información relacionada en términos de una declaración de riesgo de seguridad, estas declaraciones son expresiones en un lenguaje informal que combinan el agente, la vulnerabilidad, el objetivo vulnerable, la política violada y el activo expuesto.

Esta es una forma simple y útil para evaluaciones en menor escala donde no hay muchas declaraciones de riesgo de seguridad que efectuar. Hay que hacer notar que estas declaraciones carecen de la habilidad de expresar el impacto, la probabilidad, controles existentes, y recomendaciones.

Agente	Vulnerabilidad	Objetivo de la Vulnerabilidad	Política violada	Activo expuesto
Un hacker	Vulnerabilidades conocidas en el sistema operativo	Adquirir acceso al sistema	Para interrumpir	Servidores Web
Un intruso	Obtener acceso	A un sistema crítico	Para obtener información confidencial	Sistema crítico de presupuestos
Tormenta eléctrica	Falta protección	Daño en las comunicaciones	Perdida en la infraestructura	Enlaces inalámbricos
Empleado despedido	Omisión	Borrar información sensible	Perdida de información	Sistema contable

Tabla 3.3 Riesgos de seguridad en forma de declaraciones

A continuación se enumeran los pasos que se realizaron para el análisis de riesgos:

1. Definición del alcance
2. Identificación de posibles amenazas
3. Priorización de las amenazas
4. Impacto de la amenaza
5. Determinar el factor de riesgo
6. Identificar controles

Definición del alcance

Según Peltier (2005) cada proyecto exitoso comienza con una definición de lo que es que se va a realizar, para el análisis de riesgo va involucrar la descripción de lo que está siendo examinado. Puede ser un entorno físico como un centro de datos, un sistema específico como un sistema UNIX que soporta investigación, un elemento de procesamiento como una red de área amplia corporativa (WAN), o una sección de la red, como la red de área local de nóminas, o una aplicación específica como cuentas por pagar.

Cuando se realiza un análisis de riesgos, es necesario declarar las preocupaciones en cómo estas impactan a los objetivos del negocio o la misión de la organización, y no en como impactan a los objetivos de seguridad. Los controles apropiados son implementados porque hay una fuerte necesidad del negocio, no así que el negocio estará en el cumplimiento con los requerimientos de seguridad.

Hay que mantener durante el análisis de riesgo al negocio de la organización como lo principal en la discusión. (Peltier, 2005).

Siguiendo estas recomendaciones, el alcance del análisis de riesgo estaría delimitado al caso de estudio del trabajo de investigación, es decir, al estudio de los riesgos del entorno físico del centro de datos.

El personal de infraestructura, desarrollo de sistemas, administración de bases de datos, operarios, redes y telecomunicaciones de la organización tienen que ser parte del proceso para proporcionar la comprensión de cómo está configurado el ambiente y que controles ya están implementados.

El equipo de trabajo para la realización del análisis de riesgos de ser seleccionado de aquellos empleados con la experiencia para dar un buen conocimiento de cómo trabaja el proceso y de lo que puede ser esperado en forma de soporte. (Peltier, 2005)

De acuerdo con Peltier (2005) la calidad de la evaluación de riesgo cualitativa proviene del equipo. Un equipo conocedor proporcionará resultados de calidad.

Identificación de amenazas

De las entrevistas informales realizadas con el personal que conforma el equipo encargado de los activos de información de la organización se puede obtener un listado de las amenazas que aplican para el caso de estudio. Una vez obtenido este listado de amenazas, se define cada una de ellas de manera enlistada vea la Tabla 3.3.

Lo importante de la obtención de este listado, una vez que ha sido probado en campo, este puede ser utilizado para cualquier análisis de riesgo.

Agente	Amenaza	Definición
Natural		
	Sismo	Un repentino movimiento telúrico sea oscilatorio o trepidatorio de la tierra sea causado por fallas o por actividad volcánica.
	Huracán	Tormenta tropical con vientos sostenidos de 80 km por hora o más que se presentan en el golfo de México, más caribe, océano atlántico u océano pacífico, la cual puede caer en una clasificación o categoría de acuerdo a la velocidad de los vientos.
	Tormenta Eléctrica	Es una descarga de electricidad repentina y visible producida en respuesta a la conformación de un potencial eléctrico entre nube y suelo, entre nubes, dentro de una sola nube, o entre una nube y el aire circundante.
Ambiental		
	Fallo Eléctrico	Es una fluctuación momentánea en la fuente de alimentación eléctrica, consiste de un pico de voltaje, bajo voltaje o interrupciones de más de media hora.
	Interrupción Eléctrica	Una interrupción de largo tiempo en la fuente de alimentación eléctrica, generalmente por más de media hora.
	Fuego	Una situación que afecta a los sistemas de información a través del calentamiento, humo o daño al agente de supresión.
	Falla de hardware	Falla en una unidad o componente suficiente para causar retrasos en el procesamiento o pérdida monetaria para la empresa.
	Fuga de agua	Derrames de fuentes diferentes a la inundación. Ejemplo descompostura o fuga en tuberías, y la descarga accidental de aspersores.
	Error de software	Cualquier dado extraño o erróneo en el sistema operativo,

		aplicación que puede ocasionar errores de procesamiento, salidas de datos erróneas, o retrasos en el procesamiento.
	Interrupción de telecomunicaciones	Cualquier falla en unidades de comunicaciones o componente suficiente para causar interrupciones en la transferencia de datos vía telecomunicaciones entre computadoras e instalaciones de computo.
Deliberado por el Humano		
	Alteración de datos	Es una modificación intencional, inserción o borrado de datos, sea por usuarios autorizados o no, la cual compromete el proceso de auditoría, recuperación, disponibilidad, confidencialidad, o integridad de la información producida, procesada, controlada, o almacenada por los sistemas de procesamiento de información.
	Alteración de software	Una modificación intencional, inserción o borrado de sistema operativo o programas aplicativos, sea usuario autorizado o no, la cual compromete el proceso de auditoría, eficiencia, recuperación, disponibilidad, confidencialidad, o integridad de la información, programas, el sistema, o recursos controlados por los sistemas computacionales.
	Divulgación	La disposición intencional sin autorización o prematura de información propietaria, clasificada, confidencial de la empresa, personal o de cualquier otra forma sensitiva.
	Sabotaje	Una acción deliberada efectuada por un empleado, grupo de empleados, o persona(s) externa(s) que trabaja(n) junto con un empleado(s) para interrumpir las operaciones de la empresa.
	Fraude	Una manipulación deliberada no autorizada de hardware, software, o información con intención de ganancia financiera para el perpetrador.
	Huelga	Una acción organizada de empleados (sindicato o no, legal o no) diseñada para detener o interrumpir las operaciones normales del negocio.
	Robo	La apropiación no autorizada de hardware, software, medios, consumibles, o datos de naturaleza clasificada, pero incluida en la categoría de divulgada.
	Uso sin autorización	Uso no autorizado de equipo de cómputo o programas. Ejemplo, uso de programas personales como juegos, de inventarios, y examinar otros archivos.
	Vandalismo	La destrucción maliciosa y sin motivo o alteración de propiedad.
Accidente Humano		
	Alteración de datos	Una modificación, inserción accidental o eliminación de datos o información almacenada en los sistemas.
	Alteración de software	La modificación, inserción accidental, o borrado de sistemas operativos o programas aplicativos o porciones de código que soportan los sistemas de producción.
	Divulgación	La liberación accidental de información propietaria, clasificada, confidencial de la empresa, personal, o de

		cualquier otra manera sensitiva.
	Error de operador/usuario	Un acto accidental, impropio, o de cualquier otra forma mal escogido por un empleado que resulta en retrasos de procesamiento, daño a equipo, pérdida o modificación de datos.

Tabla 3.3 Listado de amenazas identificadas para el entorno físico del centro de datos y sus definiciones

Priorización de las amenazas

Una vez que se definieron las amenazas que se identifican de acuerdo al listado, emplearemos el formato para determinar el factor de riesgo, para determinar qué tan frecuente es la posibilidad de que ocurra cada una de las amenazas identificadas. Como es un análisis cualitativo las frecuencias se expresan como baja o alta y pueden dárseles un valor numérico aplicando los factores listados y definidos a continuación.

- **Bajo:** Totalmente improbable que la amenaza ocurra durante los próximos doce meses, toma un valor de 1.
- **Media-Bajo:** Improbable que la amenaza ocurra durante los próximos doce meses, toma un valor de 2.
- **Media:** Posible que la amenaza ocurra durante los próximos doce meses, toma un valor de 3.
- **Media-Alta:** Probable que la amenaza ocurra durante los próximos doce meses, toma un valor de 4.
- **Alta:** Muy probable que la amenaza ocurra durante los próximos doce meses, toma un valor de 5.

El valor será ingresado de acuerdo a la experiencia o los datos estadísticos que le indican que sea la posibilidad de que se presente la ocurrencia de la amenaza, si no se tiene idea de la probabilidad entonces se deja en blanco y se valora la siguiente amenaza, esto se introduce en la tabla para determinar el factor de riesgo.

Debido a que el alcance definido en el análisis fue el entorno físico se tomaran del listado de las amenazas, las que involucran el entorno físico para el caso estudiado vea la Tabla 3.4, y el dato de la posibilidad de ocurrencia es obtenido tanto de las entrevistas con el personal que labora en la organización, así como de la experiencia del investigador como criterios para la valoración.

Amenaza	Posibilidad Amenaza	Impacto	Factor de Riesgo
Tormenta Eléctrica	Media-Alta = 4		
Fallo Eléctrico	Media = 3		
Interrupción Eléctrica	Media-Alta = 4		
Fuego	Media-Bajo = 2		
Falla de Hardware	Media-Bajo = 2		
Fuga de Agua	Bajo = 1		
Error de software	Media-Bajo = 2		
Interrupción de telecomunicaciones	Media = 3		
Alteración de datos	Bajo = 1		
Alteración de software	Bajo = 1		
Divulgación	Bajo = 1		
Sabotaje	Bajo = 1		
Robo	Bajo = 1		
Uso sin autorización	Media = 3		
Error de operador/usuario	Media-Alta = 4		

Tabla 3.4 Tabla de amenazas de acuerdo a la posibilidad de que ocurra

Impacto de la amenaza

En este punto hay que estimar el impacto de pérdida si la amenaza fuera a ocurrir. El especialista debe tomar la decisión antes de hacer la revisión del impacto si las amenazas son examinadas con o sin controles existentes.

Según Peltier (2005) menciona que si el análisis de riesgo se efectúa hacia un componente de infraestructura, la amenaza es examinada como si no hubiera controles en el lugar. Para aplicaciones, sistemas y procesos de negocio la revisión se haría tomando en consideración los controles existentes.

El analista proporciona un valor de acuerdo a su experiencia o bien datos estadísticos que le indiquen el impacto al negocio, los valores que pueden ser asignados en la columna de impacto de la amenaza están descritos en la siguiente lista:

- **Bajo:** Un solo grupo de trabajo o departamento afectado; poco o muy poco impacto al proceso de negocio, toma un valor de 1.
- **Media-Bajo:** Uno o más departamentos afectados; ligero retraso en la consecución de los objetivos, toma un valor de 2.

- **Media:** Dos o más departamentos o una unidad de negocio afectada; de cuatro a seis horas de retraso en la consecución de los objetivos, toma un valor de 3.
- **Media-Alta:** Dos o más unidades de negocio afectadas; de uno a dos días de retraso en la consecución de los objetivos, toma un valor de 4.
- **Alta:** Misión entera de la empresa afectada, toma un valor de 5.

En el análisis del entorno físico procedemos a evaluar el impacto con los valores que correspondan a la amenaza planteada para la organización vea la Tabla 3.5.

Determinar el factor de riesgo

En este punto del análisis el investigador hace la suma del valor correspondiente a la posibilidad de la amenaza y el impacto de la amenaza para conseguir el factor de riesgo por cada una de las amenazas que fueron identificadas para el activo de información que está siendo analizado, en este caso el análisis de riesgo tiene el alcance del entorno físico vea la Tabla 3.5. Los factores de riesgo van a estar en el rango de bajo de dos a alto de diez.

Cuando ya se tienen todos los factores de riesgo en calificados en la tabla, el analista identifica posibles controles o protecciones para cualquier amenaza que obtenga un factor de riesgo de seis o más.

Las empresas no tienen los recursos suficientes para examinar todos los riesgos a pesar de sus factores de riesgo. Por esta razón es necesario determinar qué factores de riesgo serán identificados para una revisión posterior, los de un valor de cuatro o cinco deben ser monitoreados regularmente para asegurar que no aumente el factor de riesgo a un nivel inaceptable. Las amenazas con un factor de riesgo de tres o menos no requieren de una acción por el momento.

Amenaza	Posibilidad Amenaza	Impacto	Factor de Riesgo
Tormenta Eléctrica	Media-Alta = 4	Media = 3	7
Fallo Eléctrico	Media = 3	Media = 3	6
Interrupción Eléctrica	Media-Alta = 4	Media-Alta = 4	8
Fuego	Media-Bajo = 2	Alta = 5	7
Falla de Hardware	Media-Bajo = 2	Media-Alta = 4	6
Fuga de Agua	Bajo = 1	Media-Bajo = 2	3
Error de software	Media-Bajo = 2	Media = 3	5
Interrupción de telecomunicaciones	Media = 3	Media-Alta = 4	7
Alteración de datos	Bajo = 1	Media = 3	4
Alteración de software	Bajo = 1	Media = 3	4
Divulgación	Bajo = 1	Media = 3	4
Sabotaje	Bajo = 1	Media = 3	4
Robo	Bajo = 1	Media = 3	4
Uso sin autorización	Media = 3	Media = 3	6
Error de operador/usuario	Media-Alta = 4	Media = 3	7

Tabla 3.5 Tabla de amenazas de acuerdo al impacto que pudiera tener si se materializara la amenaza y el factor de riesgo

Identificar controles

En este punto se analizan las amenazas identificadas con un alto factor de riesgo y selecciona controles técnicos, administrativos y físicos que ofrecen un nivel aceptable de protección al activo que está siendo analizado.

Capítulo IV. Pruebas y resultados

Una vez realizado el análisis en el capítulo anterior, se procedió a la triangulación de la información obtenida en las entrevistas, la observación realizada en el lugar de la investigación y puntos de vista de autores especialistas en el área, además se identificaron controles de seguridad con respecto a la norma ISO 27002 que pueden aplicar en el centro de datos de la organización.

Los datos relevantes obtenidos, su interpretación se presentan en este capítulo.

4.1 Resultados de la encuesta y las entrevistas

Durante el desarrollo del trabajo de investigación se realizó una entrevista con el objetivo de aplicar un cuestionario al personal responsable de la organización involucrado en la operación del centro de datos, preguntas estructuradas orientadas a conocer cuál es la situación actual de la organización en materia de seguridad de la información, así también se describe la información obtenida de las entrevistas buscando guardar la identidad de las personas que participaron con la finalidad de enriquecer los resultados obtenidos en la investigación.

4.1.1 Económica (Inversión)

No existe un rubro o partida en el presupuesto asignado específicamente a la seguridad tanto física como lógica de las tecnologías de la información. La organización está consciente de la necesidad de la seguridad de la información.

Periódicamente son realizadas auditorias por consultores externos, a procesos críticos en donde también se evalúan las tecnologías de la información y comunicaciones asociadas a estos procesos, en donde incluyen algunos aspectos de seguridad de la información.

En ocasiones las recomendaciones resultado de estas auditorías son utilizadas como justificación en las adquisiciones de nuevos equipos.

A este respecto Ricardo menciona que: "Para mantener la continuidad de la operación se requiere la adquisición de un equipamiento tanto de procesamiento como de seguridad que cuente con el licenciamiento, servicio y suscripción con una vigencia de por lo menos 3 años para que en el caso de un incidente se tenga el soporte adecuado por parte del fabricante".

La adquisición de nuevos equipos en la organización tiene que estar debidamente fundamentada y justificada para ser considerada dentro del presupuesto, ya que es difícil conseguir la autorización por parte del área administrativa por las restricciones financieras actuales.

Landoll (2011) La asignación de recursos puede estar basada en riesgo de seguridad para los activos. Las organizaciones tienen recursos limitados para hacer frente a sus problemas de seguridad de la información. Si la evaluación de riesgos de seguridad no se realiza, la organización no tiene una comprensión de los riesgos de seguridad para sus activos de información. En ausencia de información sobre los riesgos de seguridad, los recursos se asignan en una variedad de otros factores, incluyendo la conveniencia, la familiaridad existente o habilidad, o simplemente por interés.

A la hora de decidir cómo gastar el presupuesto de seguridad de la información, los que toman las decisiones pueden elegir lo último en equipos ofrecidos por los proveedores que tienen una relación existente con la organización. Por lo que se observa que no existe una verdadera lista de prioridades para la inversión en tecnologías de la información.

Calder & Watkins (2008) Todos los directores, ejecutivos y gerentes, en todos los niveles en cualquier organización de cualquier tamaño, tienen que entender la forma de garantizar que sus inversiones en tecnología de la información y la información hagan posible el negocio. Cada despliegue de tecnología de la información trae consigo riesgos inmediatos para la organización, y por lo tanto cada director o ejecutivo que la despliega, o gerente que hace que cualquier uso de

la tecnología de la información debe comprender estos riesgos y los pasos que se deben tomar para contrarrestarlos.

Arnason y Willett (2008) La certificación no tiene base en requerimiento legal o reglamentario, de modo que ¿por qué molestarse? La mejor respuesta es: para validar que la inversión en los controles de seguridad cumple con los objetivos de negocio y proporciona valor de negocio.

La pregunta 18 de la encuesta efectuada al personal de la organización, revela que la razón primordial por la cual no se pone atención a la seguridad de la información, es porque no se cuenta con el presupuesto para invertir en la tecnología o el personal especializado para implementar las medidas de protección necesaria a fin de asegurar la información de la organización vea la Ilustración 4.1.

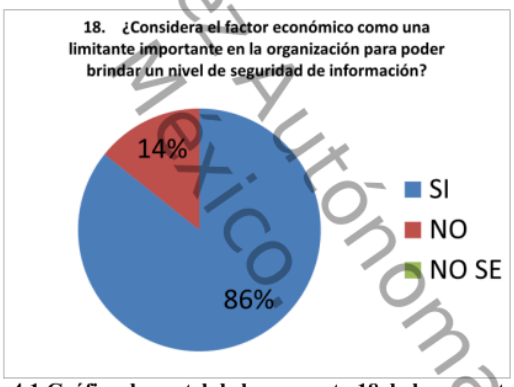


Ilustración 4.1 Gráfica de pastel de la pregunta 18 de la encuesta realizada

4.1.2 Cultura de la seguridad (capacitación, entrenamiento, conocimiento)

Los entrevistados tienen la consciencia de que es necesaria la seguridad de la información para el centro de datos ya que es el lugar donde se deposita y resguardan los datos de la organización.

Juan refiere que: “Si no se contará con la seguridad física mínima en el centro de datos como es una cerradura con llave y una cámara de vigilancia, cualquier persona ya hubiera podido entrar hasta los equipos críticos y ocasionar un incidente mayor o incluso sabotear las instalaciones”.

Ricardo comenta “En el centro de datos no existe una climatización adecuada a las necesidades de enfriamiento de los equipos ya que el ambiente es enfriado por aires acondicionado de confort que están mal ubicados, cada vez que se requiere atender un clima el personal de mantenimiento tiene que entrar hasta donde se encuentran los equipos de procesamiento y comunicación incrementando el riesgo de que se materialice una amenaza impactando a la organización”.

Jorge expresa que: “Me parece que si no se da la atención necesaria al centro de datos en cuanto a limpieza, organización, seguridad, renovación de equipos y video vigilancia. Se está en peligro de que la organización se colapse sin que se pueda garantizar la seguridad en la información”.

La organización no contempla capacitación en seguridad de la información para su personal encargado del centro de datos, día con día surgen nuevos métodos de ataque e intrusión a los sistemas que son más sofisticados y complejos.

Raúl miembro del staff que está encargado de la operación del sistema de seguridad perimetral en el centro de datos expresa que “Los firewall son equipos difíciles de operar, por ello se requiere de una capacitación especial y experiencia en el campo de la seguridad, ya que se tienen que estar monitoreando constantemente a fin de poder detectar los incidentes en la seguridad, porque no todos los equipos permiten un reporteo de los mismos”.

McIlwraith (2006) define a la cultura organizacional como un sistema de normas (valores) compartidas y creencias, o la fusión de valores individuales y de grupo, actitudes, percepciones y patrones de comportamiento. También menciona que puede ser un complejo patrón de creencias, expectaciones, ideas, valores, actitudes y comportamientos en una organización que une a sus miembros e influencia lo que ellos piensan acerca de ellos mismos y lo que hacen. Para McIlwraith la seguridad de la información tiene que ver con el comportamiento de los empleados, por ello cualquier intento de imponer una nueva cultura se encontrará con resistencia.

Según Landoll (2011) hay un crecimiento en la demanda de evaluaciones de riesgos de seguridad, pero la oferta de ingenieros experimentados en seguridad de la información para realizarlos no se ha mantenido con esa demanda.

La encuesta también revela que el personal considera que no se cuenta con una cultura de seguridad de la información en la organización.

Ilustración 4.2 Gráfica de pastel de la pregunta 12 de la encuesta realizada

4.1.3 Infraestructura (física y lógica)

Jorge operador de servidores comenta que el centro de datos no está correctamente protegido ya que las puertas del mismo son de cristal y el acceso es compartido por varias personas que tienen que realizar sus actividades de trabajo dentro del mismo espacio que ocupan los servidores y equipos de comunicación.

Ricardo miembro del staff considera que las condiciones ambientales y de limpieza no son las adecuadas para los servidores que procesan, almacenan y transmiten la información de los sistemas críticos de la organización ya que en ocasiones cuando se dañan tienen que colocar ventiladores para aliviar las necesidades de ventilación en tanto se le da mantenimiento o se sustituye el equipo.

Alejandro que es soporte técnico y entrega servicios a todas las áreas de la organización observa que existe la práctica general de manejar contraseñas muy simples, en ocasiones se divulgan la

contraseña unos a otros entre los usuarios o bien anotan las contraseñas en papelitos que dejan junto a sus computadoras para evitar olvidarla sin que estas notas estén resguardadas, incluso de sistemas de importancia para la organización. Son pocos los que recurren a solicitar el servicio de cambio de contraseña a un soporte.

Jorge considera que debería existir en las instalaciones dos o tres barreras físicas de acceso a las instalaciones del área donde se encuentran las instalaciones del centro de datos a fin de que los visitantes e incluso personal del área no tengan un fácil acceso a los servidores, almacenamientos, equipos de comunicaciones, climas y de suministro eléctrico del centro de datos.

Juan comenta que los accesos a internet están adecuadamente restringidos para los usuarios de la organización, pero que en ocasiones se hacen valer los niveles jerárquicos para obtener los permisos de uso del servicio de internet para actividades personales particulares en los equipos de la organización, incluso en dispositivos móviles.

De las observaciones realizadas en el área, se observa que el piso falso está en muy mal estado debido a la humedad, existe un piso raso totalmente cubierto por espuma de poliuretano que puede ser inflamable, no existe un sistema de detección y extinción de incendio, aún se recurre al uso de extintores manuales de gas halon, los gabinetes están descubiertos debido a la poca ventilación que tienen los servidores. Solo existen tres cámaras de video vigilancia en el área y no hay un monitoreo constante o reporte de las actividades diarias que son grabadas por las mismas.

Se observa también que dentro del centro de datos se encuentra el tablero principal de distribución eléctrica de toda el área informática por lo que si se requiere dar algún mantenimiento o realizar alguna instalación nueva los técnicos tienen que acceder a donde se encuentran los servidores para realizar su trabajo.

40

Acceso a información sensible, y a las instalaciones de procesamiento de la información, debe ser controlado y restringido a las personas específicamente autorizadas. Esto es particularmente importante para la sala de servidores, cuyo acceso debe ser muy limitado. Controles de autenticación, tales como una tarjeta magnética o códigos individuales, se debe utilizar para

autorizar y validar el acceso a las zonas seguras, y para asegurar las áreas dentro del perímetro de seguridad. Si es posible (y si es requerido por la evaluación del riesgo), el sistema de tarjeta magnética de entrada también debe proporcionar un seguimiento de auditoría de acceso. El registro de los visitantes pases emitidos se debe mantener en un lugar seguro, como puede ser que, en algún momento en el futuro, exista la necesidad de identificar a un intruso (Calder & Watkins, 2008).

Según Calder & Watkins (2008) todo el personal debe estar obligado a llevar algún tipo de identificación visible (que podría estar incorporado a una tarjeta de acceso que puede trabajar ya sea por deslizamiento o proximidad física) y deben ser encargados a detener o reportar personal ajeno no acompañado o alguien que no lleve una identificación visible. Una tarjeta de identificación visible es un control mucho más importante en una organización grande que en una pequeña, pero en cualquier tamaño de organización, visitantes no identificados y no acompañados siempre deben ser cuestionados. Hay muchas organizaciones para las cuales esto, por sí mismo, requerirá de un cambio cultural importante, y esto podría contribuir significativamente a mejorar la seguridad.

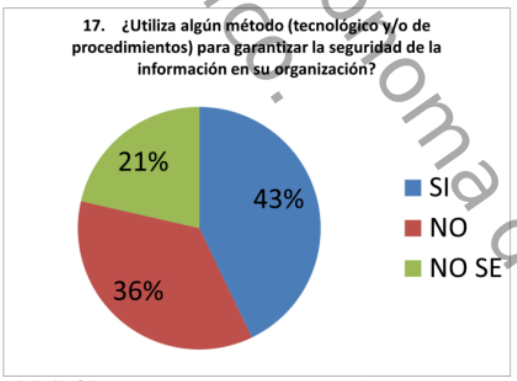


Ilustración 4.3 Gráfica de pastel de la pregunta 17 de la encuesta realizada

4.1.4 Proceso (Administración, política, procedimiento, análisis de riesgo, documentación)

No existe en los documentos oficiales un plan de contingencia, ni existe referencia a planes de contingencia en los planes de desarrollo y los programas de la organización.

Ricardo al hablar acerca de las necesidades asociadas a un plan de contingencia, mencionó:
"Me preocupa que no tengo un equipo de comunicaciones para sustituir al que estoy usando si falla, el que tengo tiene varios años en operación y no existen las refacciones necesarias para repararlo rápidamente."

Juan cuando se refería a sus equipos de almacenamiento, dijo: "Me preocupa que no contemos con discos en stock para poder reemplazar en caso de una falla y restablecer el servicio lo más pronto posible."

Alejandro como soporte refiere que existen algunos procedimientos para atender a los usuarios, pero no incorporan la práctica de la seguridad. Un ejemplo sencillo podría ser el uso de contraseñas complejas y el estarlas cambiando de manera periódica. Los usuarios no se preocupan por estas cosas y al contrario emplean contraseñas débiles o muy fáciles de encontrar, estas reglas deberían estar definidas en una política de uso de los servicios para garantizar la seguridad de la información.

Ricardo miembro del staff comenta que no se lleva a cabo un análisis de riesgo de la seguridad aun que en la organización los empleados del área están conscientes que existen amenazas y que se tienen vulnerabilidades que podrían ser explotadas impactando seriamente tanto a la operación como a la información de la organización.

Calder & Watkins (2008) mencionan que la norma claramente declara que para administrar la seguridad de la información en la organización la cláusula 6.1.1 en el anexo A de la norma ISO 27001 especifica que la administración soportará activamente la seguridad dentro de la organización a través de una clara dirección, compromiso demostrado, asignación explicita, y conocimiento de las responsabilidades de la seguridad de la información.

De los datos obtenidos en la encuesta revelan que la organización no tiene procesos de seguridad de la información y posiblemente no cuente con procedimientos basados en estándares de calidad vea la Ilustración 4.4.

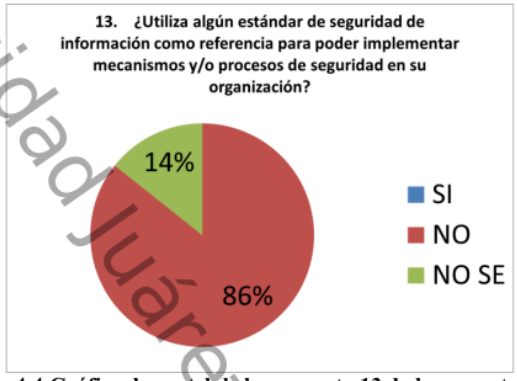


Ilustración 4.4 Gráfica de pastel de la pregunta 13 de la encuesta realizada

La encuesta también revela que al no existir proceso, procedimientos y documentación podemos afirmar que existen controles de seguridad de la información establecidos pero estos no están basados en un estándar de calidad vea la Ilustración 4.4.

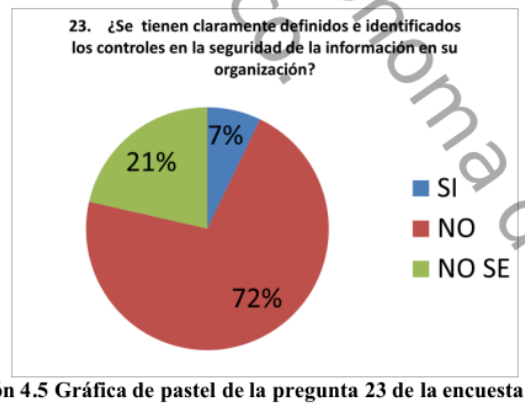


Ilustración 4.5 Gráfica de pastel de la pregunta 23 de la encuesta realizada

4.2 Recomendaciones

A partir de los ejes de análisis identificados del cruce de la evaluación organizacional, con los hallazgos obtenidos en este capítulo se proponen las recomendaciones o controles de la norma ISO 27002 y son presentados en la Tabla 4.1.

Eje de Análisis	Controles de la norma ISO 27002
1. Inversión **Hallazgos** **-Bajos presupuestos** **-Falta de asignación de prioridad en las necesidades de TI**	Los proyectos de TI con frecuencia representan inversiones significativas de recursos financieros y gerenciales. El interés de los accionistas en la efectividad de tales despliegues debe ser reflejado en la transparencia con la cual son planeados, administrados, medidos, y la forma en la cual los riesgos son evaluados y controlados. La seguridad de la información es la protección de la información ante una gran variedad de amenazas con el fin de asegurar la continuidad del negocio, minimizar el riesgo para el negocio y maximizar el retorno de inversiones y oportunidades para el negocio. La información y los procesos, sistemas y redes que la soportan son activos importantes de negocio. La definición, el logro, el mantenimiento y la mejora de la seguridad de la información pueden ser esenciales para mantener su competitividad, el flujo de caja, la rentabilidad, el cumplimiento legal y la imagen comercial.
2. Cultura de la seguridad **Hallazgos** **- Falta de capacitación** **- Desconocimiento de rol o responsabilidad** **- Ausencia de una política de seguridad.**	Controles específicos que la organización puede adoptar para revertir la situación actual en cuanto a la cultura de la seguridad. 5.1. La alta dirección deberá evidenciar su compromiso para el establecimiento de una política de seguridad. 5.2.2 La organización deberá asegurar que a todo el personal que se le han asignado responsabilidades dentro del SGSI sea competente para desempeñar tales actividades, determinando las competencias o proporcionando la capacitación, manteniendo los registros de educación, entrenamiento, especialidades, experiencia y calificaciones. 6.1.1 La Gerencia deberá apoyar activamente la seguridad dentro de la organización mediante una dirección clara, compromiso demostrado, delegación explícita, y reconocimiento de las responsabilidades de seguridad de la información. 8.2.2 Todo el personal de la organización y, cuando sea pertinente, los contratistas y usuarios de terceros, deberán recibir el entrenamiento de concientización adecuado y actualizaciones periódicas de políticas y procedimientos de la organización, según corresponda a sus funciones de trabajo. 13.2.1 Deberán establecerse responsabilidades y procedimientos de gerencia para asegurar la respuesta rápida, efectiva y ordenada a los incidentes de seguridad de la información.
3. Infraestructura **Hallazgos** **-Falta de medidas de seguridad física**	La seguridad de la información es importante tanto para los negocios del sector público como del privado y para proteger la infraestructura crítica. En ambos sectores, la seguridad de la información actuará como un elemento facilitador para lograr, por ejemplo, gobierno en línea (e-goverment) o negocios electrónicos (e-business) y evitar o reducir los riesgos pertinentes.
4. Procesos **Hallazgos**	5.1 Asegurando que se establezcan objetivos y planes del SGSI, establecimiento de funciones y responsabilidades, comunicar a la organización la importancia de alcanzar los objetivos de seguridad de la información, proporcionar los recursos suficientes, definir

-Falta de procedimientos y documentación del proceso	criterios de aceptación de riesgo. 5.2.1. Asegurar que los procedimientos de seguridad de la información apoyen los requerimientos de negocio, mantener la seguridad adecuada mediante la aplicación correcta de los controles implementados, realizar revisiones cuando sea necesario y reaccionar debidamente ante los resultados de estas revisiones.

Tabla 4.1 Recomendaciones de la norma ISO 27002 con respecto a los ejes de análisis y los hallazgos obtenidos de la evaluación organizacional

4.3 Mitigación de Riesgos y selección de controles

Según Landoll (2011), la evaluación del riesgo de seguridad el valor de los activos de información, mide la fortaleza de toda la planeación de la seguridad, y proporciona la información necesaria para hacer mejoras planeadas basadas en los riesgos de seguridad de la información. Es la herramienta para la administración que le proporciona una medida eficaz de sus controles de seguridad y un indicador de que tan bien están protegidos sus activos.

Actualmente la mayoría de las organizaciones están incorporando la evaluación del riesgo de seguridad en sus planes de seguridad de la información como una manera de mejorar continuamente sus controles y permanecer en cumplimiento las regulaciones de seguridad de la información.

El plan de tratamiento de riesgo provee la orientación de cómo la organización controlará cada riesgo. Lo cual puede incluir el ignorar, aceptar, compartir, transferir o mitigar cada riesgo. El punto es producir un plan que especifique la acción y proporcionar una razón detrás de cada acción. (Arnason & Willet, 2008).

11

La selección de los controles de seguridad depende de las decisiones de la organización basadas en los criterios para la aceptación del riesgo, el tratamiento del riesgo y el enfoque general para la administración del riesgo aplicado en la organización, y debería estar sujeta a toda la legislación y todos los reglamentos nacionales e internacionales pertinentes.

Algunos controles en la norma ISO 27002 pueden considerarse como principios guía para la gestión de la seguridad de la información y son aplicables para la mayoría de las organizaciones.

La norma ISO 27002 en el punto 4.2 que es tratamiento del riesgo establece que antes de que se considere el tratamiento del riesgo, la organización debería decidir los criterios para determinar si se pueden aceptar o no los riesgos. Los riesgos si se pueden aceptar, por ejemplo, si se evaluó que el riesgo es bajo o que el costo del tratamiento no es eficiente económicamente factible para la organización. Estas decisiones de la organización deben ser registradas.

Para cada uno de los riesgos identificados después de la evaluación de riesgos es necesario tomar una decisión para su tratamiento. Las opciones posibles son:

a. aplicar los controles apropiados para reducir los riesgos;
b. aceptar objetivamente y conscientemente los riesgos, siempre y cuando satisfagan la política de la organización y sus criterios para la aceptación del riesgo;
c. evadir los riesgos al no permitir acciones que pudieran causar que el riesgo ocurra;
d. transferir los riesgos asociados a otros, por ejemplo aseguradoras o proveedores.

Los controles se pueden seleccionar a partir de la norma, de otros conjuntos de controles, o se pueden diseñar controles nuevos que satisfagan las necesidades específicas de la organización. (ISO 27002, 2005).

Debe de considerar que no hay conjunto de controles que pueda lograr una seguridad completa, y que debería ser implementada una administración adicional para monitorear, evaluar, mejorar la eficiencia y eficacia de los controles de seguridad para apoyar las metas de la organización.

Selección de controles de acuerdo a la norma ISO 27002

Los controles son protecciones para mitigar los riesgos. La selección de los controles correctos es esencial para la protección de los activos y para disminuir el factor de riesgo.

Con el propósito de certificarse en la norma ISO 27001, seleccione los controles del estándar ISO 27002 que apliquen a la organización. Observe que algunos controles de seguridad necesarios para la organización pudieran no estar en ISO 27002, también hay que notar que para obtener la certificación en ISO 27001 no requiere la implementación de todos los controles. Lo que si

requiere es un conocimiento total y conciencia de los riesgos, justificación para las acciones o posturas hacia el riesgo. (Arnason & Willett, 2008).

Para Arnason & Willett (2008) cuando se seleccionan controles de acuerdo al resultado de la evaluación de riesgo, el objetivo es reducir o eliminar la vulnerabilidad y por lo tanto reducir el riesgo. Seleccione los controles que pueden reducir el impacto y ayudar con la recuperación si una amenaza ocurre.

En la Tabla 3.5 se presenta el resultado de la evaluación o análisis de riesgos realizado en el capítulo 3, en donde se observa el listado de las amenazas detectadas para el caso estudiado valorando de manera cualitativa la posibilidad de la amenaza, el impacto y determinando el factor de riesgo por cada amenaza.

Los factores de riesgo que tienen un valor ordinario de seis o más están marcados en gris ya que son los que requieren atención inmediata, siendo que el factor de riesgo más alto fue de 8 lo cual nos está indicando que una interrupción eléctrica es una amenaza potencial que de ocurrir pudiera tener un impacto mayor en la organización, sea económico, social, político, de imagen, de confianza, etc.

Para poder minimizar o mitigar el riesgo con respecto a la norma ISO 27002 se propone a la organización una selección de controles mostrados en la Tabla 4.2 y posteriormente son descritos en la Tabla 4.3.

Estos controles o recomendaciones pudieran ser factibles de implementación por la organización, en algunos casos la protección requiere de una inversión en equipos. Para el caso estudiado si la organización tuviera la posibilidad económica, existen soluciones como son plantas de emergencia, sistemas de energía ininterrumpible, reguladores, bancos de batería que permitirían a la organización mitigar el impacto de que la amenaza ocurra.

Amenaza	Posibilidad Amenaza	Impacto	Factor de Riesgo	Controles seleccionados
Tormenta Eléctrica	Media-Alta	Media	7	9.2.1
Fallo Eléctrico	Media	Media	6	9.2.2
Interrupción Eléctrica	Media-Alta	Media-Alta	8	9.2.2
Fuego	Media-Bajo	Alta	7	9.1.4
Falla de Hardware	Media-Bajo	Media-Alta	6	9.2.4, 10.10.5
Fuga de Agua	Bajo	Media-Bajo	3	9.1.4
Error de software	Media-Bajo	Media	5	10.4.1, 12.4.1, 12.6.1
Interrupción de telecomunicaciones	Media	Media-Alta	7	9.2.2, 9.2.3, 10.10.5
Alteración de datos	Bajo	Media	4	10.5.1, 10.6.1, 10.6.2, 11.2.1
Alteración de software	Bajo	Media	4	10.5.1, 10.6.1, 10.6.2
Divulgación	Bajo	Media	4	6.1.5, 6.2.2, 8.1.1, 9.2.6, 10.7.2, 10.7.3, 10.7.4, 11.2.3
Sabotaje	Bajo	Media	4	9.1.1, 9.1.2, 9.1.4
Robo	Bajo	Media	4	8.3.2, 9.1.1, 9.1.2, 9.2.7
Uso sin autorización	Media	Media	6	7.1.3, 8.1.1, 9.2.6, 10.7.3, 10.7.4
Error de operador/usuario	Media-Alta	Media	7	7.1.3, 10.5.1, 10.6.1, 10.7.2, 10.10.4

Tabla 4.2 Identificación de los controles basado en la norma ISO 27002 de acuerdo al análisis de riesgo

Los controles seleccionados para disminuir el impacto si se presentan las amenazas se describen a continuación de acuerdo a su numeración en el estándar ISO 27002 en la Tabla 4.3 de acuerdo al análisis de riesgos efectuado al entorno físico de la organización bajo estudio.

Ref.	Control	Descripción del control	Amenazas del caso de estudio
6.1.5	Convenios de confidencialidad	Los requerimientos de convenios de confidencialidad o de no divulgación que reflejen las necesidades de la organización para protección de la información deberán ser identificados y revisados periódicamente.	- Divulgación
6.2.2	Enfocar la seguridad en el trato con los clientes	Control Deberán enfocarse todos los requisitos de seguridad identificados antes de darles a los clientes acceso a la información o activos de la organización	- Divulgación
7.1.3	Uso aceptable de los activos	Deberán identificarse, documentarse e implementarse reglas para el uso aceptable de la información y de los activos relacionados con las instalaciones de procesamiento de	- Uso sin autorización - Error de operador/usuario

		información.	
8.1.1	Funciones y responsabilidades	Las funciones y responsabilidades de seguridad de los empleados, contratistas y usuarios de terceros deberán definirse y documentarse de acuerdo a la política de seguridad de información de la organización.	- Uso sin autorización
8.3.2	Devolución de activos	Todos los empleados, contratistas y usuarios de terceros deberán devolver todos los activos de la organización en su poder al terminar su empleo, contrato o convenio.	- Robo
9.1.1	Perímetro de seguridad física	Se deberían utilizar perímetros de seguridad (barreras tales como paredes, puertas de acceso controladas con tarjeta o mostradores de recepción atendidos) para proteger las áreas que contienen información y servicios de procesamiento de información.	- Sabotaje - Robo
9.1.2	Controles de acceso físico	Las áreas seguras deberían estar protegidas con controles de acceso apropiados para asegurar que sólo se permite el acceso a personal autorizado.	- Sabotaje - Robo
9.1.4	Protección contra amenazas externas y ambientales	Se deberían diseñar y aplicar protecciones físicas contra daño por incendio, inundación terremoto, explosión, manifestaciones sociales y otras formas de desastre natural o artificial.	**- Fuego** - Fuga de Agua - Sabotaje
9.2.1	Ubicación y protección de los equipos	Los equipos deberían estar ubicados o protegidos para reducir el riesgo debido a amenazas o peligros del entorno, y las oportunidades de acceso no autorizado.	**- Tormenta eléctrica**
9.2.2	Servicios de suministro	Los equipos deberían estar protegidos contra fallas en el suministro de energía y otras anomalías causadas por fallas en los servicios de suministro.	**- Fallo eléctrico** **- Interrupción eléctrica** - Interrupción de telecomunicaciones
9.2.3	Seguridad del cableado	El cableado de energía y telecomunicaciones que conduzca datos o soporte los servicios de	- Interrupción de telecomunicaciones

		información deberá estar protegido de intercepción o daño.	
9.2.4	Mantenimiento de los equipos	Los equipos deberían recibir mantenimiento adecuado para asegurar su continua disponibilidad e integridad.	**- Falla de hardware**
9.2.6	Seguridad en la reutilización o eliminación de los equipos	Se deberían verificar todos los elementos del equipo que contengan medios de almacenamiento para asegurar que se haya eliminado cualquier software licenciado y datos sensibles o asegurar que se hayan sobrescrito de forma segura, antes de la eliminación.	- Divulgación - Uso sin autorización
9.2.7	Remoción de propiedad	No se sacará equipo, información o software fuera de las instalaciones sin previa autorización.	- Robo
10.4.1	Controles contra código malicioso	Deberá implementarse controles de detección, prevención y recuperación para protegerse contra código malicioso así como procedimientos adecuados de concientización de usuarios.	- Error de software
10.5.1	Respaldo de la información	Deberán hacerse copias de respaldo de la información y el software, y probarse periódicamente según la política de respaldo convenida.	- Alteración de datos - Alteración de software
10.6.1	Controles de redes	Las redes deberán manejarse y controlarse debidamente, a fin de protegerse de amenazas, y mantener la seguridad de los sistemas y aplicaciones que usan la red, incluyendo la información en tránsito.	- Alteración de datos - Alteración de software - Error de operador/usuario
10.6.2	Seguridad de los servicios de red	Las características de seguridad, niveles de servicio, y requisitos de gestión de todos los servicios de red deberán identificarse e incluirse en cualquier convenio de servicios de red, ya sea que los servicios se provean internamente o del exterior.	- Alteración de datos - Alteración de software

10.7.2	Eliminación de medios	Los medios deberán eliminarse de modo seguro y sin riesgo de accidente cuando no se les necesite más, usando procedimientos formales	- Error de operador/usuario
10.7.3	Procedimiento de manipulación de información	Deberán establecerse procedimientos para la manipulación y almacenamiento de información, a fin de protegerla de la divulgación no autorizada o del mal uso.	- Divulgación - Uso sin autorización
10.7.4	Seguridad de la documentación del sistema	Deberá protegerse la documentación del sistema contra el acceso no autorizado	- Uso sin autorización
10.10.4	Registros de Administrador y operador	Se deberán registrar las actividades del administrador del sistema y del operador del sistema.	- Error de operador/usuario
10.10.5	Registro de fallas	Las fallas deberán registrarse, analizarse y deberán tomarse las medidas adecuadas.	**- Falla de hardware** - Interrupción de telecomunicaciones
11.2.1	Inscripción de usuarios	Deberá haber un procedimiento formal de inscripción y des-inscripción de usuarios para otorgar y revocar el acceso a todos los sistemas y servicios de información.	- Alteración de datos
11.2.3	Manejo de contraseña de usuarios	La asignación de contraseñas deberá controlarse mediante un proceso de manejo formal.	- Divulgación
12.4.1	Control del software operativo	Deberán existir procedimientos para controlar la instalación de software en los sistemas operativos.	- Error de software
12.6.1	Control de vulnerabilidades técnicas	Deberá obtenerse información oportuna sobre las vulnerabilidades técnicas de los sistemas de información en uso, evaluarse la exposición de la organización a esas vulnerabilidades, y tomarse medidas adecuadas para resolver el riesgo relacionado	- Error de software

Tabla 4.3 Controles seleccionados con su descripción para mitigar el riesgo de que ocurra la amenaza

Capítulo V. Conclusiones y trabajos futuros

Podemos concluir que la seguridad de la información es un tema que la organización debe tener muy en cuenta a la hora de adoptar nuevas tecnologías, desarrollar sus propios sistemas de información e interconectar redes de voz y datos con otras dependencias e incluso con el mundo exterior. Un buen punto de partida para el aseguramiento de la información puede ser el adoptar una administración de riesgos de seguridad, efectuar evaluación de riesgos de seguridad de la información de manera periódica y realizar una planeación estratégica de las tecnologías de la información y comunicaciones.

Las normas internacionales como la ISO 27000 dicen que hacer para implementar un sistema de gestión de seguridad de la información pero no dicen cómo hacerlo, tampoco limitan a la organización a emplear una sola metodología o una sola herramienta, en este sentido la organización es libre de escoger la forma en cómo llevar a cabo la implementación e incluso de adoptar ciertos controles de acuerdo a su tamaño, a sus objetivos, a su economía, en fin a sus necesidades.

Es importante que la organización ponga especial cuidado al tema de la cultura de la seguridad, ya que el comportamiento de los empleados puede ocasionar serios daños en los activos de información, o bien puede existir la resistencia en la adopción de nuevas tecnologías. La selección del personal, los requerimientos de seguridad y la capacitación del mismo son fundamentales para que se logren los objetivos de seguridad planteados por la organización.

Aunque los presupuestos actualmente son muy austeros se deben priorizar las necesidades de seguridad de la información de la organización, no solo de las áreas de tecnologías de la información sino toda la organización. Los mecanismos o controles de protección física para las instalaciones, el monitoreo y vigilancia de las instalaciones, mayor inversión en sistemas de detección y extinción de incendios, plantas de emergencia, supresores, reguladores, sistemas de

energía ininterrumpible, tableros y bancos de baterías para los equipos en los centros de datos, climatización adecuada para centros de cómputo ya que los aires de confort en ocasiones alivian la situación por un corto periodo y generalmente tienden a fallar en cuanto más se les necesita.

Se debe re evaluar los procesos de la organización que involucran las tecnologías de la información y comunicaciones para introducir el tema de la seguridad de la información, para que los altos niveles de la estructura organizacional tengan la tarea de definir la política de seguridad que se deberá de aplicar de acuerdo a los objetivos, misión y visión de la organización.

Las áreas de tecnologías de información deberán definir los procedimientos, lineamientos y reglamentos en materia de seguridad de la información conforme a la norma, estableciendo y monitoreando los controles para medir su efectividad.

Si bien la certificación en la norma no es una prioridad actualmente para la organización, documentando sus procesos de seguridad, estableciendo una política y procedimientos de seguridad podrá contar con un buen camino avanzado en esa dirección que le permitirán en el corto plazo estar en conformidad con la norma y tal vez en el futuro optar por la certificación lo cual le dará una mayor ventaja competitiva a la organización y un reconocimiento a nivel nacional e internacional.

La organización tiene la posibilidad de evaluar y analizar los riesgos de seguridad, partiendo de este punto tiene la posibilidad de decidir cómo tratar con esos riesgos, ya sea eliminándolo, transfiriéndolo, aceptarlo o minimizarlo de acuerdo a lo establecido por la organización.

Trabajos futuros

Trabajos futuros que pueden llevarse a cabo a partir de esta investigación puede ser una evaluación de la seguridad de la información de toda la organización, una evaluación del cambio organizacional con respecto a la seguridad de los activos de información, la implementación de la norma ISO 27001, el diseño de una política de seguridad, el establecimiento de una administración de riesgos, o bien una evaluación de los riesgos de seguridad empleando herramientas software de prueba tanto intrusivas como no intrusivas.

Referencias

AENOR. (2010). Asociación Española de Normalización y Certificación: Normalización. Recuperado el 1 de Junio de 2010, de http://www.aenor.es/desarrollo/normalizacion/quees/europa.asp

Aguilera, P. (2010). Seguridad Informática. España: Editex.

Alger, D. (2005). Build the Best Data Center Facility for Your Business. USA: Cisco Press.

American Psychological Association (2010). The Basics of APA Style. Recuperado Mayo, 3 2010 de: http://flash1r.apa.org/apastyle/basics/index.htm

Arnason, S. & Willet, K. (2008). How to achive 27001 certification. USA: Auerbach Publications.

Calder, A. (2009). Implementing Information Security Based on ISO 27001/27002 – A Management Guide. Van Haren Publishing.

Calder, A., & Watkins, S. (2008). IT governance: a manager's guide to data security and ISO 27001/ISO 27002 (4th ed.). USA: Kogan Page.

Carvajal, A. (2007, Agosto). GLOBALTEKSECURITY. Obtenido de Tecnologías globales para la seguridad de la información: http://www.acis.org.co/fileadmin/Articulos/TecnicasAtaqueComputacionForense.pdf

Clepner, K. J., & Gutiérrez, T. A. (31 de marzo de 2002). Administración y Ejecución de un Plan Estratégico de Tecnología de Información. Recuperado el 6 de Marzo de 2010, de http://www.revista.unam.mx/vol.3/num1/art1/

Corletti Estrada, A. (Abril de 2006). Análisis de ISO-27001:2005. Recuperado el 6 de Marzo de 2010, de http://www.kriptopolis.org/docs/iso.pdf

Cresson, W. C. (2002). Políticas de seguridad informática – Mejores prácticas internacionales. (S.d.C.A, Trad.), Houston, Texas, USA: NetIQ. Inc.

Del Rio G. C., Del Río S. C., & Del Río S. R. (2009). El presupuesto: generalidades, tradicional, áreas y niveles de responsabilidad, programas y actividades, base cero, teoría y práctica (10 ed.). D.F., México: Cengage Learning.

Erbschloe, M. (2005). Physical security for IT. USA: Elsevier.

Ernst & Young (2009, Junio 11). Encuesta la seguridad en México. *b:Secure* (J. Hernández Sosa, Ed.) Obtenido de http://www.bsecure.com.mx/ultimos-articulos/ernst-young-encuesta-la-seguridad-en-mexico/

Flórez, A. (2008). Metodología para la creación de una arquitectura de seguridad informática. Recuperado el 1 de Marzo de 2010. Obtenido de http://150.187.25.30/descargas/Walc2008/seguridad/CONFERENCIAS/Metodologia%20para%20la%20creaci%D0%B2n%20de%20arquitecturas%20de%20seguridad%20inform%D0%B0tica.pdf

Gómez, A. (2007). Enciclopedia de la seguridad informática. (1ra ed).D.F., México: Alfaomega.

Hernández S. R., Fernández C. C., & Baptista L. P. (2006). Metodología de la investigación (4ed.). México: McGraw Hill.

Herrmann, D. S. (2002). A practical guide security engineering and information assurance. Auerbach Publications.

Hill, D. G. (2009). Data Protection: Governance, Risk Management, and Compliance. Boca Raton, Florida, USA: Auerbach Publications.

International Organization for Standardization. (2010). International Standards for business, government and society. Recuperado, Noviembre, 10 de 2010, de http://www.iso.org/

International Organization for Standardization. (2010). Understand the basics. Recuperado el Mayo de 2010, de http://www.iso.org/iso/iso_catalogue/management_standards/understand_the_basics.htm

ISO (2005). ISO/IEC FDIS 27001:2005. ISO/IEC.

Jayaswal, K. (2006). Administering Data Centers: Servers, Storage, and Voice over IP. Indianapolis, Indiana, USA: Wiley Publishing.

Koontz, H., & Weihrich, H. (2006). Essentials Of Management (7 ed.). Tata McGraw-Hill.

Landoll, D. (2011). The Security Risk Assessment Handbook A Complete Guide for Performing Security Risk Assessments (2nd. ed.). USA. CRC Press.

Ley del Impuesto Sobre la Renta. (2010). Nueva Ley publicada en el Diario Oficial de la Federación del 1º de enero de 2002, texto vigente que contempla las últimas reformas publicado en el Diario Oficial de la Federación del 27 de abril de 2010. Recuperado el 1 de Junio de 2010, de http://www.cddhcu.gob.mx/LeyesBiblio/pdf/82.pdf

López T. M., & Correa O. J. I. (2007). Planeación estratégica de tecnologías informáticas y sistemas de información (1ra ed.). Manizales, Colombia: Universidad de Caldas.

Martínez, J. (2001). Introducción al análisis de Riesgos. D.F., México: LIMUSA.

McIlwraigth, A. (2006). Information security and employee behaviour: how to reduce risk through employee education, training and awareness. England. Gower Publishing.

42

Morón L. E. (2002). Internet y derecho penal: "hacking" y otras conductas ilícitas en la red. Aranzadi.

Muñoz R. C. (2002). Auditoria en Sistemas Computacionales. México: Pearson Educación.

Organization for Economic Co-operation and Development. (25 de Julio de 2002). OECD Guideline for the Security of Information Systems and Networks: Towards a Culture of Security. Recuperado el 6 de Marzo de 2010, de http://www.oecd.org/document /42/ 0,3343,en_2649_34255_15582250_1_1_1_1,00.html

Patton, M. Q. (2002). Qualitative research and evaluation methods. (3rd. ed.). Thousand Oaks, California, USA: Sage Publications, Inc.

Peltier, T. (2002). Information security policies, procedures, and standards: guidelines for effective information security management. Boca Raton, Florida, USA:CRC Press.

Peltier, T. (2005). Information security risk analysis (2 ed). Boca Raton, Florida, USA:CRC Press.

Política Digital. (2009, Junio 16). Taller Nacional Seguridad de la Información en el Sector Público de México. *Política Digital.* Recuperado Mayo de 2010, de Conclusiones: http://www. politicadigital.com.mx/?P=leernoticia&Article=2334

Política Digital. (20 de Mayo de 2010). Lectura Sugerida. Recuperado el Mayo de 2010, de Hacia una nueva transparencia en México: Apertura y Seguridad: http://aperturayseguridad2010. politicadigital.com.mx/lectura.html

Real Academia Española. (2001). Diccionario de la lengua española (22 ed.). Madrid: Espasa Calpe.

Rodríguez, G., Gil, J., y García, E. (1999). Metodología de la investigación cualitativa. España: Alabrije.

Rodríguez, N., & Martínez, W. (2006). Planificación y Evaluación de Proyectos Informáticos (3ra. ed.). San José, Costa Rica: Editorial de la Universidad Estatal a Distancia.

Schmelkes, C. (1998). Manual para la presentación de anteproyectos e informes de investigación: (tesis) (2 ed.). D.F., México: Oxford University Press.

Snevely, R. (2002). Enterprise Data Center Design and Methodology. USA: Prentice Hall PTR.

Tecnológico de Monterrey. (s.f.). Formato APA. Obtenido de http://serviciosva.itesm.mx/cvr/formato_apa/categorias.htm

Vacca, J. R. (Ed.). (2009). Computer and Information Security Handbook. USA: Elsevier.

Vasilachis, I. (2006). Estrategias de investigación cualitativa. España: Editorial Gedisa.

Weil, S. (22 de Diciembre de 2004). How Itil can improve information security. Recuperado el 6 de Marzo de 2010, de Whitepaper: http://www.symantec.com/connect/articles/how-itil-can-improve-information-security

Wylder, J. (2004). Strategic Information Security. USA: Auerbach Publications.

Xuanzi, H., & Cunxi, X. (2006). Security Operation Center Design Based on D-S Evidence Theory. Mechatronics and Automation, Proceedings of the 2006 IEEE International, 2302-2306.

Glosario de siglas

AENOR:	Asociación Española de Normalización y Certificación.
APA:	American Psychological Association.
BS:	British Standard.
CEPAL:	Comisión Económica para América Latina.
DAIS:	División Académica de Informática y Sistemas.
EE.UU:	Estados Unidos de América.
JTC:	Join Technical Committe.
ISO:	International Standardization Organization.
IEC:	International Electrotechnical Commission.
OCDE:	Organización para la Cooperación y Desarrollo Económico.
PDCA:	Plan-Do-Check-Act.
PERT:	Planned Evaluation and Review Technique.
PHCA:	Planear-Hacer-Comprobar-Actuar.
SGSI:	Sistema de Gestión de la Seguridad de la Información.
TICS:	Tecnologías de la Información y Comunicaciones.
UJAT:	Universidad Juárez Autónoma de Tabasco.
USA:	United States of America.

Anexo A. Presupuestos que integran el costo total del trabajo recepcional.

PRESUPUESTO DE MATERIALES DE OFICINA

Para la elaboración de éste presupuesto se cotizaron precios al 1 de Junio de 2010, en la empresa Ofix, ubicada en Plaza San Luís, a continuación se muestra el presupuesto que se generó:

PRESUPUESTO DE MATERIALES DE OFICINA				
Descripción	**Unidades**	**Cantidad**	**Costo Unitario**	**Costo Total**
Hojas	Paquete (500)	4	48.00	192.00
Sobres	Pieza	25	2.00	50.00
Bolígrafos	Pieza	5	2.50	12.50
Lápices	Pieza	10	3.50	35.00
Marca texto	Pieza	5	5.00	25.00
Copias	Pieza	1000	0.30	300.00
Impresiones	Pieza	750	1.00	750.00
Cartuchos	Pieza	3	250.00	750.00
USB	Pieza	2	150.00	300.00
Cd's	Pieza	5	10.00	50.00
			Total	**$2,464.50**

PRESUPUESTO DE MANO DE OBRA INTELECTUAL Y VIATICOS

Este presupuesto contempla tanto la mano de obra intelectual como los viáticos necesarios para elaborar la investigación.

Para determinar el costo diario del investigador se consideró $90.00 pesos MN.

Referente a los viáticos considerados para la realización de la investigación éstos contemplan gastos de transporte y alimentación. Para su determinación se estimó un costo promedio de

conceptos anteriormente señalados en los lugares a los cuales se tendrá que trasladar el investigador.

A continuación se presenta tanto el presupuesto de mano de obra intelectual como el desglose de los viáticos.

PRESUPUESTO DE MANO DE OBRA INTELECTUAL			
Descripción	**Sueldo diario**	**Días que requieren costo**	**Total**
Investigación	$90.00	260	$23,400.00
Viáticos			500.00
		Totales	**$23,900.00**

DESGLOSE DE VIÁTICOS	
Pasajes	300
Gasolina	1000
Alimentación	500
Total	**$1,800.00**

PRESUPUESTO DE DEPRECIACIÓN DE ACTIVOS FIJOS

Para la elaboración de éste presupuesto se aplicaron los porcentajes anuales de depreciación que establece la Ley del Impuesto Sobre la Renta según lo establece art. 40 fracción VII, el cual señala: "30%..... Cómputo" (LISR pág. 51).

El costo que se asignó a los activos fijos propiedad del investigador que serán utilizados para elaborar la investigación, corresponde al costo real estimado de acuerdo a las condiciones en que se encuentran. A continuación se presenta el presupuesto correspondiente.

PRESUPUESTO DE DEPRECIACIÓN DE ACTIVOS FIJOS				
Equipo	**Inversión**	**Depreciación anual 30%**	**Depreciación diaria**	**Días que requieren costo 181**

Computadora Portátil	$16,000.00	**$4,800.00**	**$13.15**	**$2,380.27**
Impresora Láser B/N	1,000.00	**300.00**	**0.82**	**148.77**
			Totales	**$2,529.04**

PRESUPUESTO DE ENERGÍA ELÉCTRICA E INTERNET

Para determinar el costo de éstos conceptos se obtuvo el costo promedio diario que se paga por los mismos en la casa del investigador, y posteriormente se determinó un costo estimado que fuera aplicable a la investigación, quedando el presupuesto como se muestra a continuación:

PRESUPUESTO DE ENERGÍA ELÉCTRICA E INTERNET		
Conceptos	**Costo diario Promedio**	**Costo total** Días Investigación **181**
Energía eléctrica	2.50	$452.50
Internet	6.75	1,221.75
	Total	**$1,674.25**

PRESUPUESTO DE DERECHOS DE TITULACIÓN

Para determinar estos costos se acudió al Coordinador de estudios Terminales para pedirle orientación respecto a los costos actuales que cobra la UJAT por los diferentes derechos de titulación, teniendo así que el presupuesto queda como se menciona a continuación.

PRESUPUESTO DE DERECHOS DE TITULACIÓN	
Descripción	**Costo unitario**
Derechos de Examen profesional	14515
Derechos de Centro de computo	500
Pago de Servicios bibliotecarios	400
Certificado de Estudio de Maestría y Carta de Terminación	400
Recibo de pago de examen	2000
Constancia de comprensión de textos en inglés	350
Total	**$18,165.00**

PRESUPUESTO DE IMPRESIÓN Y EMPASTADO

Para la elaboración de este presupuestos se investigó en centros de copiado ubicados en la DAIS el costo actual de las copias e impresiones tanto en blanco y negro como en color, igualmente se acudió a varias imprentas de la ciudad de Villahermosa a cotizar los empastados con diferentes materiales de los cuales se seleccionó el que el investigador considero pertinente y se determinó un costo promedio.

PRESUPUESTO DE IMPRESIÓN Y EMPASTADO				
	No. de	Hojas por	Costo	
CONCEPTOS	tesis	tesis	Unitario	Importe
Impresiones originales	1	120	$1.00	$120.00
Fotocopias	11	120	0.30	396.00
Empastado	12		100.00	1,200.00
			Total	**$1,716.00**

PRESUPUESTO DE NORMAS ISO

Para elaborar este presupuesto se tomaron los costos de la página (http://www.itgovernance.co.uk/standards.aspx) y el tipo de cambio para la libra esterlina al día 7 de Junio de 2010 que es de 18.7705 pesos por libra tomado de la página (http://es.exchange-rates.org/Rate/GBP/MXN).

PRESUPUESTO DE ADQUIRIR LAS NORMAS ISO	
Descripción	Costo unitario
ISO/IEC 27001:2005 (ISMS specification)	$1,689.35
ISO/IEC 27002:2005 (Code of Practice)	$2,064.76
ISO/IEC 27005: 2005 (Information Security Risk Management)	$1,689.35
Total	**$5,443.46**

ESTIMACIÓN DEL TIEMPO, CRONOGRAMA DE ACTIVIDADES

En este apartado se presenta el tiempo necesario para concluir la investigación, cabe mencionar que para la estimación de los costos se aplicó La Técnica de Revisión y Evaluación de Programas [Planned Evaluation, and Review Technique] (PERT), para terminar la investigación en la fase de trabajo recepcional (Elaboración de la investigación) poder cumplir con los objetivos establecidos y alcanzar los resultados comprometidos.

Rodríguez y Martínez (2006), mencionan que PERT es un modelo para la administración y gestión de proyectos inventado en 1958 por la Oficina de Proyectos Especiales de la Marina de Guerra del Departamento de Defensa de los EE. UU. Consiste básicamente en un método para analizar las tareas involucradas para completar un proyecto determinado, especialmente el tiempo para completar cada tarea, e identificar el tiempo mínimo necesario para completar el proyecto total. Su aplicación se basa en la siguiente fórmula:

$$Te = \frac{to + 4tn + tp}{6}$$

Dónde:

Te= Tiempo esperado

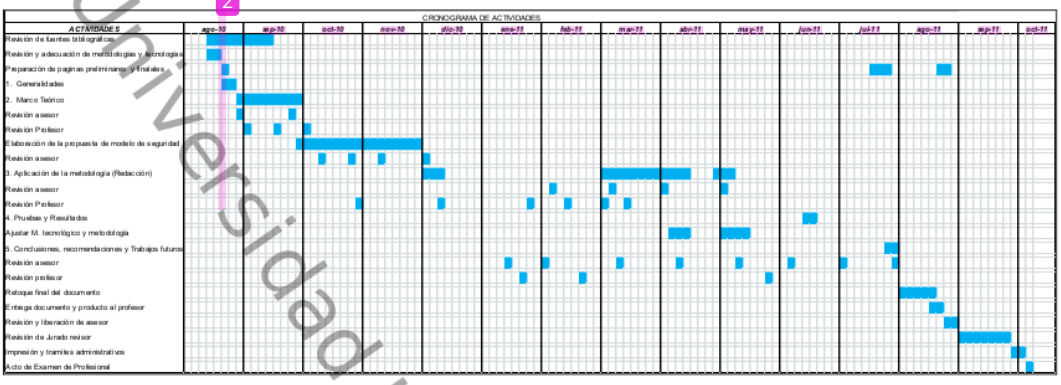
To= Tiempo optimo

Tn= Tiempo normal

Tp= Tiempo pesimista

Para la aplicación de PERT se asignó tiempo a las actividades contempladas en el trabajo de investigación, además se consideraron otras actividades a realizar, que requieren tiempo y/o costo y que no se describen en el índice como son: revisión de fuentes y pulido final del documento.

A continuación se muestra la gráfica de los tiempos estimados resultados de la aplicación de la técnica PERT por medio del cronograma del trabajo.



ESTIMACIÓN DE COSTOS DE LA INVESTIGACIÓN

Es conveniente que los costos totales que se esperan para el desarrollo de la investigación, se presentan mediante una tabla en el trabajo, y en los anexos se presenten los diferentes presupuestos que integran el costo total, así como los criterios seguidos para su formulación.

En este apartado se muestra el costo total que se estima para la investigación, cabe destacar que para su determinación se utilizó la técnica de presupuesto. Un presupuesto es un cálculo anticipado de los ingresos y gastos de una actividad económica (personal, familiar, un negocio, una empresa, una oficina, una investigación) durante un periodo de tiempo. Se considera un plan de acción dirigido a cumplir una meta prevista, expresada en valores y términos financieros que, debe cumplirse en determinado tiempo y bajo ciertas condiciones previstas. Del Río G. C., Del Río S. C., y Del Río S. R. (2009), mencionan que un presupuesto puede considerarse como una parte clásica del ciclo administrativo que consiste en planear, actuar y controlar o, más específicamente, como una parte, de un sistema total de administración.

El costo total de la investigación asciende a la cantidad de $57,692.25 como se aprecia en la Tabla.

COSTO TOTAL DE LA INVESTIGACIÓN	
Descripción	**Importe**
Materiales de oficina	$2,464.50
Mano de obra intelectual	$25,700.00
Depreciación de activos fijos	$2,529.04
Energía eléctrica e Internet	$1,674.25
Derechos de titulación	$18,165.00
Impresión y empastado	$1,716.00
Adquisición de normas ISO	$5,443.46
Totales	**$57,692.25**

Anexo B. Cuestionario

UNIVERSIDAD JUÁREZ AUTÓNOMA DE TABASCO
DIVISIÓN ACADÉMICA DE INFORMÁTICA Y SISTEMAS

Estimado lector:
Estoy realizando un estudio sobre la seguridad de la información en su organización, es por ello que le solicito atentamente su colaboración para aplicar un cuestionario el cual me permitirá recolectar los datos para un análisis con fines de investigación, para realizar mi tesis de posgrado en Administración de Tecnologías de la Información en la Universidad Juárez Autónoma de Tabasco, División Académica de Informática y Sistemas, los datos obtenidos serán de carácter confidencial y las encuestas totalmente anónimas.

Por favor conteste las siguientes preguntas marcando con una X dentro del cuadrado que corresponda, y complemente su respuesta según sea requerido en la pregunta.

☐ Directivo de TI ☐ Operativo de TI ☐ Usuario dentro del área de TI

1. ¿Comprende el concepto de "seguridad de la información"?

   ☐ Si ☐ No ☐ No sé
2. ¿Considera necesaria la seguridad de la información en el centro de procesamiento de datos de su organización?

   ☐ Si ☐ No ☐ No sé
3. ¿Cuenta su organización con alguna certificación de acuerdo a la norma ISO o cualquier otra norma internacional en materia de seguridad de la información actualmente?

   ☐ Si ☐ No ☐ No sé
4. ¿Está en vías de implementar algún sistema de gestión de calidad, de acuerdo a una norma nacional o internacional?

   ☐ Si ☐ No ☐ No sé

   En caso de que la respuesta a la pregunta sea **SI** escriba sobre la siguiente línea que norma se va a implementar, si la respuesta es **No** o **No sé** continúe en la siguiente pregunta.

   _____

5. ¿Considera necesario desarrollar una política de seguridad de la información en su organización?

   ☐ Si ☐ No ☐ No sé

6. ¿Existen en la organización políticas y procedimientos de control de seguridad en las tecnologías de información?

   ☐ Si ☐ No ☐ No sé

7. ¿Se tienen bien definidas, documentadas y establecidas las políticas de seguridad de información en la organización?

   ☐ Si ☐ No ☐ No sé

8. ¿Existe un área o personal dedicado a la seguridad en tecnologías de información en la organización?

   ☐ Si ☐ No ☐ No sé

   En caso de que su respuesta sea **No o No sé**, pase a la pregunta 11

9. ¿El área de seguridad de la información apoya o soporta las estrategias y la misión de su organización?

   ☐ Si ☐ No ☐ No sé

10. ¿El personal encargado de la seguridad de la información es suficiente para cubrir las necesidades de la organización?

    ☐ Si ☐ No ☐ No sé

11. ¿La alta dirección apoya y se encuentra involucrada con el área o personal de tecnologías de la información para la seguridad de la información de la organización?

    ☐ Si ☐ No ☐ No sé

12. ¿Prevalece en toda la organización una cultura de seguridad de la información?

    ☐ Si ☐ No ☐ No sé

13. ¿Utiliza algún estándar de seguridad de información como referencia para poder implementar mecanismos y/o procesos de seguridad en su organización?

    ☐ Si ☐ No ☐ No sé

    En caso de que la respuesta a la pregunta sea **SI** escriba sobre la línea cual es el estándar que emplea y después continúe en la pregunta **15**, si la respuesta es **NO** o **No sé** pase a la pregunta siguiente.

    _____

14. ¿Sus clientes han expresado la necesidad de implementar un estándar de seguridad en las TI en su empresa?

    ☐ Si ☐ No ☐ No sé

15. ¿Se cuenta en la organización con un plan de contingencia escrito en caso de posibles ataques informáticos?

    ☐ Si ☐ No ☐ No sé

16. ¿Se ha detectado algún intento de Intrusión a la organización en los últimos tres años, ya sea realizado por personal interno o externo a la organización?

☐ Si ☐ No ☐ No sé

17. ¿Utiliza algún método (tecnológico y/o de procedimientos) para garantizar la seguridad de la información en su organización?

☐ Si ☐ No ☐ No sé

18. ¿Considera el factor económico como una limitante importante en la organización para poder brindar un nivel de seguridad de información?

☐ Si ☐ No ☐ No sé

19. ¿Se cuenta con un programa de capacitaciones para el personal que está involucrado con la seguridad de la información?

☐ Si ☐ No ☐ No sé

20. ¿Es difundida la importancia de la seguridad de la información en su organización?

☐ Si ☐ No ☐ No sé

21. ¿Se realizan auditorias de seguridad dentro de su organización?

☐ Si ☐ No ☐ No sé

22. ¿Se tienen definidas métricas de seguridad de la información en su organización?

☐ Si ☐ No ☐ No sé

23. ¿Se tienen claramente definidos e identificados los controles en la seguridad de la información en su organización?

☐ Si ☐ No ☐ No sé

24. ¿Cómo evaluarías la seguridad de la información en la organización?

☐ (1) Muy Bien ☐ (2) Bien ☐ (3) Regular ☐ (4) Mal ☐ (5) Muy Mal

25. ¿Cómo evaluarías la seguridad física en el centro de datos?

☐ (1) Muy Bien ☐ (2) Bien ☐ (3) Regular ☐ (4) Mal ☐ (5) Muy Mal

26. ¿Cómo evaluarías la seguridad lógica en el centro de datos?

☐ (1) Muy Bien ☐ (2) Bien ☐ (3) Regular ☐ (4) Mal ☐ (5) Muy Mal

27. ¿Cómo evaluarías las condiciones en que se encuentra la infraestructura del centro de datos?

☐ (1) Muy Bien ☐ (2) Bien ☐ (3) Regular ☐ (4) Mal ☐ (5) Muy Mal

28. ¿Considera ud. que su organización en el corto o mediano plazo debería apegarse a una norma internacional para la seguridad de la información?

☐ (1) Muy Bien ☐ (2) Bien ☐ (3) Regular ☐ (4) Mal ☐ (5) Muy Mal

Muchas gracias por su tiempo y su apoyo.

PLANEACION EN LA SEGURIDAD DE LA INFORMACIÓN PARA CENTROS DE DATOS EN ORGANIZACIONES DE GOBIERNO

ORIGINALITY REPORT

14%
SIMILARITY INDEX

PRIMARY SOURCES

1	cip.org.pe Internet	402 words — 2%
2	docplayer.es Internet	297 words — 1%
3	gmas2.envigado.gov.co Internet	198 words — 1%
4	cryptomex.org Internet	144 words — 1%
5	archivos.ujat.mx Internet	142 words — 1%
6	portafolioresumenaudinformatica.blogspot.com Internet	122 words — 1%
7	ri.ues.edu.sv Internet	112 words — 1%
8	es.wikipedia.org Internet	94 words — < 1%
9	www.coursehero.com Internet	83 words — < 1%
10	www.iso27000.es Internet	80 words — < 1%

11	nor27002eva.blogspot.com Internet	79 words — < 1%
12	www.ptolomeo.unam.mx:8080 Internet	78 words — < 1%
13	repositorio.tec.mx Internet	68 words — < 1%
14	biblioteca.utb.edu.co Internet	64 words — < 1%
15	hdl.handle.net Internet	58 words — < 1%
16	documents.mx Internet	52 words — < 1%
17	www.slideshare.net Internet	50 words — < 1%
18	1library.co Internet	48 words — < 1%
19	www.compute-rs.com Internet	46 words — < 1%
20	repository.ean.edu.co Internet	44 words — < 1%
21	prezi.com Internet	35 words — < 1%
22	repository.unad.edu.co Internet	35 words — < 1%
23	www.bcrsistemas.com.ar Internet	35 words — < 1%

24	repository.usta.edu.co Internet	34 words — < 1%
25	sites.google.com Internet	34 words — < 1%
26	vsip.info Internet	31 words — < 1%
27	fdocuments.mx Internet	30 words — < 1%
28	www.extrememeters.com Internet	30 words — < 1%
29	fdocumentos.tips Internet	29 words — < 1%
30	pt.slideshare.net Internet	29 words — < 1%
31	banca4finanzas.files.wordpress.com Internet	28 words — < 1%
32	repositorio.espe.edu.ec Internet	28 words — < 1%
33	www.clubensayos.com Internet	28 words — < 1%
34	repository.unilibre.edu.co Internet	27 words — < 1%
35	virtual.urbe.edu Internet	26 words — < 1%
36	bibdigital.epn.edu.ec Internet	21 words — < 1%

37	repositorio.ug.edu.ec Internet	21 words — < 1%
38	www.emagister.com.mx Internet	21 words — < 1%
39	ciencia.lasalle.edu.co Internet	20 words — < 1%
40	es.slideshare.net Internet	20 words — < 1%
41	www.buenastareas.com Internet	19 words — < 1%
42	www.eumed.net Internet	17 words — < 1%
43	core.ac.uk Internet	16 words — < 1%
44	pdfcoffee.com Internet	16 words — < 1%
45	www.orgsolidarias.gov.co Internet	15 words — < 1%

EXCLUDE QUOTES	ON	EXCLUDE SOURCES	OFF
EXCLUDE BIBLIOGRAPHY	ON	EXCLUDE MATCHES	< 15 WORDS