Escuela de Graduados

Monografía para Optar por el Título de:

Maestría en Gerencia y Productividad

Propuesta de Implementación de la Norma ISO 27001:2005 Grupo PCDATA TECHNOLOGIES en la ciudad de Santo Domingo 2013

Sustentante:

Pedro M. Castillo R. **2011-0670**

Asesor (a):

Edda Freites Mejia, MBA

Santo Domingo, Rep. Dom.
Agosto, 2013

RESUMEN

RESUMEN

Este trabajo de investigación presenta una descripción de los fundamentos de la norma ISO 27001 y su aplicación en las organizaciones. Como caso práctico se presenta una experiencia de implementación de la norma en una organización, esta norma puede ser implantada en una empresa con el objetivo de obtener la certificación o simplemente como mejores prácticas para perfeccionar algunos aspectos de seguridad en la empresa. Adicionalmente se indica cómo implementar estas buenas prácticas en empresas pequeñas que no pueden realizar la certificación. El hecho de disponer de la certificación ayuda a gestionar y proteger sus valiosos activos de información. ISO 27001 es la única norma internacional auditable que define los requisitos para un sistema de gestión de la seguridad de la información (SGSI). La norma se ha concebido para garantizar la selección de controles de seguridad adecuados y proporcionales. Ello ayuda a proteger los activos de información y otorga confianza a las partes interesadas, sobre todo a los clientes. La norma adopta un enfoque por procesos para establecer, implantar, operar, supervisar, revisar, mantener y mejorar un SGSI. La norma es particularmente interesante si la protección de la información es crítica, como en finanzas, sector público y tecnología de la información (TI). ISO 27001 Puede utilizarse para garantizar a los clientes que su información está protegida.

INDICE

ÍNDICE DE CONTENIDO

CAPITULO III.
PROPUESTA DE IMPLEMENTACION DE LA NORMA ISO 27001:2005 DE LA EMPRESA PCDATA TECHNOLOGIES.

INDICE DE TABLAS

INDICE DE FIGURAS

INTRODUCCION

INTRODUCCION

El propósito de la seguridad de información es asegurar la continuidad del negocio y minimizar daños a la firma previniendo y minimizando el impacto de incidentes de seguridad. La gestión de seguridad de información permite que la información sea compartida, asegurando la protección de la información y todos los activos comprendidos en el alcance del sistema.

Un sistema de gestión de seguridad de información (SGSI) tiene tres componentes para alcanzar confidencialidad y aseguramiento de la información:

- **Confidencialidad:** protección de la información sensitiva de intercepciones no autorizadas.

- **Integridad:** La propiedad de salvaguardar la exactitud e integridad de los activos.

- **Disponibilidad:** La propiedad de estar disponible y utilizable cuando lo requiera.

Según el British Standard Institute es una estructura probada para la gestión y mejora continua de las políticas, los procedimientos y procesos de la organización. Las empresas que operan en el siglo XXI se enfrentan a muchos retos, significativos, entre ellos: Rentabilidad, competitividad, globalización, velocidad de los cambios, capacidad de adaptación, crecimiento y tecnología.

Equilibrar estos y otros requisitos empresariales puede constituir un proceso difícil y desalentador. Es aquí donde entran en juego los sistemas de gestión, al permitir aprovechar y desarrollar el potencial existente en la organización. En la actualidad uno de los principales activos que las organizaciones poseen, es la información. Por lo cual es necesario que toda

organización que busque una excelencia en los servicios o productos que ofrece, adopte una Sistema de Gestión para el manejo adecuado de la información, garantizando así su disponibilidad, confidencialidad e integridad. En el presente trabajo final se pretende explicar de forma ordenada el estudio realizado en una empresa acerca de la implementación de la norma ISO 27001:2005, dividido en tres capítulos cuyo contenido es el siguiente:

- En el capítulo 1, se aborda sobre los aspectos generales de la norma ISO 27001:2005, las principales teorías que regulan la norma, así como también las técnicas y métodos utilizados hoy en día.

- En el capítulo 2, se hace una investigación más detallada en la empresa bajo investigación, con la finalidad de establecer el perfil de la situación actual y las posibles fallas.

- En el capítulo 3, por su parte, se establece una propuesta de mejora de la situación existente dentro de la empresa. Las recomendaciones planteadas en dicho capítulo pretenden con su implementación cambiar el panorama actual dentro de la misma.

Toda organización que desee convertirse en un proveedor confiable debería garantizar la continuidad de su negocio ante posibles escenarios de amenazas que pudieran presentarse.

CAPITULO I.

Definición de Seguridad de la Información

CAPITULO I.
DEFINICIÓN DE SEGURIDAD DE LA INFORMACIÓN

La información de la empresa es uno de los activos más importantes que poseen y tiene un valor para la organización y por lo tanto se debería desarrollar mecanismos que aseguren una protección adecuada. Los objetivos de la seguridad de la información son proteger a la organización de amenazas, minimizar los años y maximizar el retorno de las inversiones y las oportunidades del negocio.

En vista de que la información de una organización puede adoptar diversas formas, como: escrita en papel, impresa, almacenada electrónicamente, transmitida por correo o por medios electrónicos, mostrada en vídeo o hablada electrónicamente. Debería protegerse adecuadamente cualquiera que sea la forma que tome o los medios por los que se comparta o almacene.

La seguridad de la información consiste en la preservación de su confidencialidad, integridad y disponibilidad:

Confidencialidad:

Acceso a la información por parte únicamente de quienes están autorizados.

Integridad:

Mantenimiento de la exactitud y completitud de la información y sus métodos de procesos.

Disponibilidad:

Acceso a la información y sus activos asociados por parte de los usuarios autorizados cuando lo requieran.

La seguridad de la información se consigue implantando un conjunto apropiado de controles, que pueden ser políticas, procedimientos, estructuras organizativas y funciones de software. El objetivo de estos controles es asegurar que se cumplen con los requisitos de seguridad de la información.

1.1 Gestión de Riesgos

1.1.1 Introducción

La gestión del riesgo es una parte fundamental de la Norma ISO 27001. Los Controles en el anexo A del estándar deberían ser seleccionados en base a los resultados de la evaluación del riesgo, se requiere medir y evaluar los riesgos así como revisar y reevaluar los riesgos en una etapa futura para asegurar que se tiene implantando una eficaz seguridad de información.

Ya que los controles son seleccionados en base a los resultados de la gestión de riesgo, es claro que si una empresa no está bien informada sobre los riesgos no podrá alcanzar una efectiva gestión de control.

1.1.2 Definición de Riesgo[1]

Riesgo es el daño potencial que puede surgir por un proceso presente o evento futuro.

Diariamente en ocasiones se lo utiliza como sinónimo de probabilidad, pero en el asesoramiento profesional de riesgo, el riesgo combina la probabilidad de que ocurra un evento negativo con cuánto daño dicho evento Causaría.

1.1.3 Fuentes de Riesgo

Hay distintas fuentes las cuales pueden tener un impacto en la organización. Una fuente es llamada amenaza.

[1] Albts, C. y Dorofee, A. (2005). Managing Information Security Risk. Pearson Education.

Una amenaza tiene el potencial de causar un incidente no deseado, el cual puede provocar daños al sistema, la organización y a los activos. Pueden ser amenazas de la naturaleza, accidentes causados por negligencia o amenazas intencionales causadas por acciones maliciosas. Para que una amenaza cause daño tendría que explorar la vulnerabilidad del Sistema, aplicación o servicio.

Ilustración 1. Fuentes de Riesgo.

Fuentes: British Standard Institute , http://www.aspectosprofesionales.info/2013/05/implantacion-de-un-sgsi-adoptando-la.html

1.1.4 Análisis del Riesgo

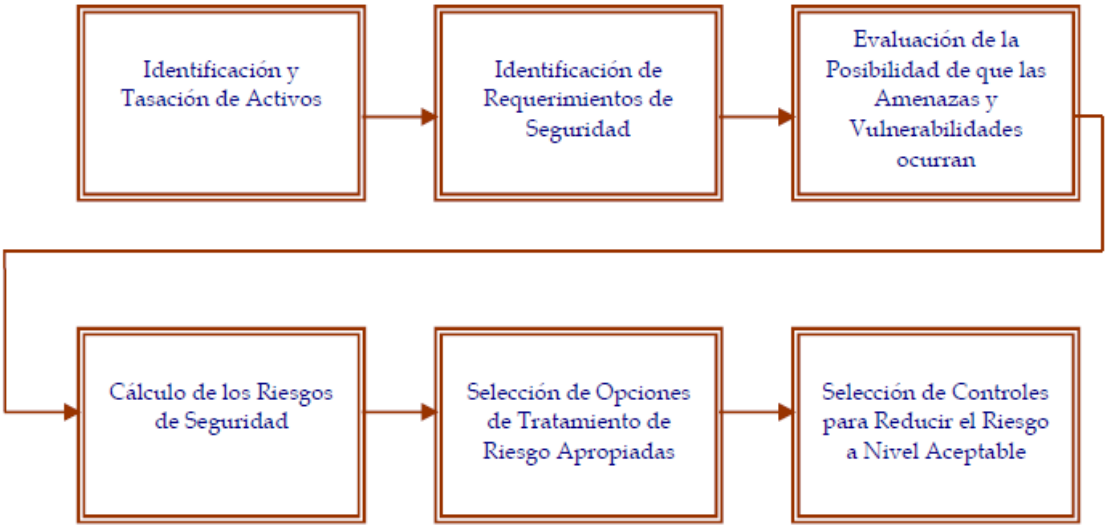
Para implantar un Sistema de Gestión de Seguridad de Información según ISO 27000, la organización requiere determinar el alcance del estándar en la empresa, y en base a ese alcance identificar todos los activos de información. Luego es requerido un análisis de riesgo para identificar qué activos están bajo riesgo. El objetivo del análisis del riesgo es apreciar la magnitud del riesgo que afecta a los activos de la información.

Es deber de la gerencia revisar el S GSI a intervalos planificados para asegurar su adecuación y eficacia, ya que ISO 27001:2005 es un sistema dinámico que obliga a la gerencia estar constantemente revisando y definiendo controles, sus amenazas, vulnerabilidades e iniciar acciones correctivas y preventivas cuando sea necesario.

1.1.5 Proceso de Evaluación del Riesgo

La figura 2 muestra el proceso de evaluación del riesgo que permite a una organización estar en conformidad con los requerimientos del estándar ISO 27001.

Ilustración 2. Proceso de evaluación del Riesgo.



Fuente: Barnes, J. (2005). A Guide to Business Continuity Planning. Wiley.London

Identificación y tasación de activos[2]

Cada activo debe estar claramente identificado y valorado apropiadamente, y su propietario y clasificación de seguridad acordada en la organización. El ISO 17799:2005 (Código de Práctica para la Gestión de la Seguridad de Información) clasifica los activos de la siguiente manera:

[2] Alexander, A. (2007). Diseño de un sistema de gestión de seguridad de información. Alfaomega

1) De información: bases de datos y archivos de datos, documentación del sistema, manuales de usuario, materiales de entrenamiento, procedimientos operativos de apoyo, planes de continuidad.

2) Documentos impresos: documentos impresos, contratos, lineamientos, documentos de la compañía, documentos que contienen resultados importantes del negocio.

3) Activos físicos: Equipos de comunicación y computación, medios magnéticos, otros equipos técnicos.

4) Personas: Personal, clientes, suscriptores.

5) Imagen y reputación de la compañía.

6) Servicios: Servicios de computación y comunicación, otros servicios Técnicos.

Identificación de requerimientos de seguridad

Con el objetivo de identificar los requisitos de seguridad de la organización, es aconsejable basarse en las tres fuentes principales, que se describen a continuación:

a) La primera fuente es derivada de la valoración de riesgos de la organización. Con ella se identifica las amenazas a los activos, se evalúa las vulnerabilidades y la probabilidad de su ocurrencia.

b) La segunda fuente es el conjunto de requisitos legales, estatutos, regulaciones y contratos que debería satisfaces la organización, sus socios comerciales, los contratistas y los proveedores de servicios.

c) La tercera fuente está formada por los principios, objetivos y requisitos que forman parte del tratamiento de la información que la organización ha desarrollado para apoyar sus operaciones.

Identificación de amenazas y vulnerabilidades

Las vulnerabilidades son debilidades asociadas con los activos de la empresa. Las debilidades pueden ser explotadas por las amenazas, causando incidentes no deseados, que pudieran terminar causando pérdidas, daño o deterioro a los activos.

La vulnerabilidad como tal, no causa daño, es simplemente una condición o conjunto de condiciones que pueden permitir que una amenaza afecte a un activo.

Cálculo de los riesgos de seguridad[3]

El propósito de la evaluación del riesgo es el de identificar y evaluar los riesgos. La evaluación de riesgo es una consideración consecuente:

Consecuencias[4]

Del impacto económico que probablemente resulte de un fallo de seguridad, teniendo en cuenta las posibles consecuencias de pérdida de confidencialidad, integridad o disponibilidad de la información y otros activos;

Probabilidad[5]

La probabilidad realista de que ocurra dicho fallo a la luz de las amenazas y vulnerabilidades existentes, así como de los controles implantados. Los resultados de esta evaluación ayudarán a dirigir y determinar una adecuada acción gerencial y las prioridades para gestionar los riesgos de seguridad de la información, y la implantación de los controles adecuados para protegerse contra dichos riesgos. El proceso de evaluación de riesgos y selección de controles, pueden requerir que sea realizado varias veces para cubrir partes diferentes de la organización o sistemas de información individuales.

[3] Aceituno, V. (2006); Information Security Management Maturity Model. ISM3. ISECOM.
[4] Idem.
[5] Idem.

Es importante, efectuar revisiones periódicas de los riesgos de seguridad y de los controles implantados para:

- Tener en cuenta los cambios de los requisitos y las prioridades de negocio de la organización.

- Considerar nuevas amenazas y vulnerabilidades.

- Confirmar que las medidas de control siguen siendo eficaces y apropiadas.

1.2 Selección de Opciones para el Tratamiento del Riesgo

Cuando los riesgos han sido identificados y evaluados, la organización debería identificar y evaluar la acción más apropiada para tratar los riesgos, lo que se conoce como el Plan de Tratamiento de Riesgos (PTR), que es un documento o conjunto de ellos, de vital importancia para el SGSI.

El objetivo fundamental es describir de forma bien clara las actualizaciones que se van a realizar para disminuir los riesgos a niveles aceptables, qué recursos van a asignarse para la realización de cada una de estas actualizaciones, las responsabilidades asociadas y las posibles prioridades en la ejecución de las actualizaciones.

1.2.1 Reducción del riesgo

Para los riesgos donde la opción de reducirlos ha sido escogida, se deben implementar los apropiados controles para disminuirlos a los niveles de aceptación previamente identificados por la empresa.

Al identificar los controles a ser implantados es importante considerar los requerimientos de seguridad relacionados con el riesgo, así como las vulnerabilidades y las amenazas previamente identificadas.

Los controles pueden reducir los riesgos valorados en varias maneras:

- Reduciendo la posibilidad de que la vulnerabilidad sea explotada por las amenazas.

- Reduciendo la posibilidad de impacto si el riesgo ocurre detectando eventos no deseados, reaccionando o recuperándose de ellos.

- La elección de cualquiera de estas maneras para controlar los riesgos dependerá de una serie de factores, tales como: requerimientos comerciales de la organización, el ambiente, y las circunstancias en que la firma requiere operar.

- Un aspecto muy importante que se debe tomar en cuenta si la empresa opta por este método para el tratamiento del riesgo, es el económico.

1.2.2 Aceptación del riesgo[6]

Es probable que a la empresa se le presente situaciones donde no se pueden encontrar controles ni tampoco es viable diseñarlos o el costo de implantar el control es mayor que las consecuencias del riesgo. En estas circunstancias una decisión razonable pudiera ser la de inclinarse por la aceptación del riesgo, y vivir con las consecuencias si el riesgo ocurriese.

1.2.3 Transferencia del riesgo

La transferencia del riesgo, es una opción para la empresa, cuando es muy difícil, tanto técnica como económicamente para la organización llevar al riesgo a un nivel aceptable. En estas circunstancias podría ser económicamente factible, transferir el riesgo a una aseguradora. Hay que tomar en cuenta, que con las empresas aseguradoras, siempre existe un elemento de

[6] Alexander Alberto Ph.D , Diseño de un Sistema de Gestión de Seguridad, Editorial Alfaomega, Colombia, 2007

riesgo residual. Siempre existen condiciones con las aseguradoras de exclusiones, las cuales se aplicarán dependiendo del tipo de ocurrencia, bajo la cual no se provee una indemnización. La transferencia del riesgo por lo tanto, debe ser muy bien analizada para así poder identificar con precisión, cuánto del riesgo actual está siendo transferido. Otra posibilidad es la de utilizar a terceras partes para el manejo de activos o procesos considerados críticos. En la medida en que la empresa tercializadora esté preparada para asumir dicha responsabilidad. Lo que debe estar claro, es que al tercerizar servicios, el riesgo residual no se delega, es responsabilidad de la empresa.

1.2.4 Evitar el riesgo.[7]

La opción de evitar el riesgo, describe cualquier acción donde las actividades del negocio, o las maneras de conducir la gestión comercial del negocio, se modifican, para así poder evitar la ocurrencia del riesgo.

- Las maneras habituales para implementar esta opción son:
- Dejar de conducir ciertas actividades.
- Desplazar activos de información de un área riesgosa a otra.
- Decidir no procesar cierto tipo de información si no se consigue la protección adecuada.

La decisión por la opción de "evitar el riesgo" debe ser balanceada contra las necesidades financieras y comerciales de la empresa.

1.2.5 Selección de controles para reducir los riesgos a un nivel aceptable.[8]

Para reducir el riesgo evaluado dentro del alcance del SGSI considerado, controles de seguridad apropiados y justificados deben ser identificados y seleccionados. La selección de controles debe ser sustentada por los resultados de la evaluación del riesgo.

[7] Alexander Alberto Ph.D , Diseño de un Sistema de Gestión de Seguridad, Editorial Alfaomega, Colombia, 2007
[8] Idem.

Las vulnerabilidades con las amenazas asociadas indican donde la protección pudiera ser requerida y qué forma debe tener. Cuando se seleccionan controles para la implementación, un número de factores deben ser considerados:

- Uso de controles
- Transparencia del usuario
- Ayuda otorgada a los usuarios para desempeñar su función
- Relativa fuerza de controles
- Tipos de funciones desempeñadas

1.2.6 Riesgo Residual

Una vez que las decisiones del tratamiento del riesgo han sido implementadas, siempre habrá un riesgo residual. Es necesario calcular cuánto las decisiones del tratamiento del riesgo ayudan a reducir el riesgo, y cuánto queda de riesgo residual.

El riesgo residual es definido como “aquel riesgo que queda en la empresa después de haber implementado el plan de tratamiento del riesgo”.

El riesgo residual es muchas veces difícil de calcular, pero por lo menos un estimado debe ser determinado. En el caso de que el riesgo residual no fuera aceptable, una decisión gerencial debe ser tomada para resolver la situación. Una opción es la de identificar diferentes opciones de tratamiento del riesgo, incrementar los controles, o establecer arreglos con aseguradoras, para finalmente poder reducir el riesgo a un nivel aceptable.

Es importante estar claros, que una buena práctica es la de no tolerar riesgos inaceptables, pero en algunas circunstancias, podría ser necesario tener que aceptarlos. Los riesgos residuales que son aceptados, deben ser documentados y aprobados por la gerencia.

1.3 Controles de un Sistema de Seguridad de la Información. 6

ISO 27001 contiene un anexo A, que considera los controles de la norma ISO 17799 para su posible aplicación en SGSI que implante cada organización.

1.3.1 Estructura del Sistema de Gestión.[9]

Un Sistema de Gestión es una herramienta de la que dispone la Gerencia para dirigir y controlar un determinado ámbito. Las empresas tienen la posibilidad de implantar un número variable de estos Sistemas de Gestión para mejorar la organización y beneficios sin imponer una carga a la organización. Los Sistemas de Gestión se aplican en el marco de todas las actividades que se ejecutan en la organización y son válidos solo si cada uno de ellos interactúa con los demás armónicamente.

La estructura de los Sistemas de Gestión debe ser tal que sea factible realizar una coordinación y un control ordenado y permanente sobre la totalidad de las actividades que se realizan. Deben estructurarse y adaptarse al tipo y características de cada organización, tomando en consideración particularmente los elementos que sean apropiados para su estructuración; para lo cual se debe definir:

- Estructura Organizativa.
- Resultados deseables que se pretenden lograr.
- Procesos que se llevan a cabo para cumplir con la finalidad.
- Procedimientos mediante los cuales se ejecuta las actividades y tareas.

El objetivo de los estándares de Gestión de ISO es llegar a un único Sistema de Gestión que contemple todos los aspectos necesarios para la organización, basándose en el ciclo PDCA y el proceso de mejora continua.

[9] Alexander Alberto Ph.D , Diseño de un Sistema de Gestión de Seguridad, Editorial Alfaomega, Colombia, 2007

1.3.2 Operatividad de los Sistemas de Gestión.[10]

Los Sistemas de Gestión adaptados al tipo particular de organización, debe operar de tal manera que se dé la confianza apropiada; es decir que: Sean bien comprendidos por la totalidad de los protagonistas, operan en forma eficaz, los resultados satisfacen las expectativas de las partes interesadas, se enfatiza las acciones preventivas ante cualquier clase de problemas

1.4 Normas Iso, 27001:2005.[11]

1.4.1 Historia.[12]

Durante más de un siglo, el Instituto Británico de Normas Técnicas (BSI) y la Organización Internacional de Normas Técnicas (ISO) han brindado 3 parámetros globales a las normas técnicas de operación, fabricación y desempeño. Solo faltaba que BSI e ISO propusieran una norma técnica para la seguridad de la información.

En 1995, el BSI publicó la primera norma técnica de seguridad; la BS 7799, la cual fue redactada con el fin de abarcar los asuntos de seguridad relacionados con el e–commerce. La Norma se consideraba inflexible y no tuvo gran acogida. No se presentó la norma técnica en un momento oportuno y los problemas de seguridad no despertaron mucho interés en ese entonces. En Mayo de 1999, el BSI intentó de nuevo publicar su segunda versión de la Norma BS 7799, la que fue una revisión más amplia de la primera publicación. En Diciembre del 2000, La ISO adoptó y publicó la primera parte de su norma BS 7799 bajo el nombre de ISO 17799. En Septiembre del 2002 se publicó BS 7799 – 2; en esta revisión se adoptó el “Modelo de Proceso” con el fin de alinearla con ISO 9001 e ISO 14001. El 15 de Octubre del 2005 se aprueba la Norma ISO 27001:2005 y en 2006 existen más de 2030 compañías certificadas a nivel mundial.

[10] http://www.iso27000.es/sgsi.html
[11] Idem.
[12] Idem.

1.4.2 Definición de las normas iso 27000.[13]

La serie ISO 27000 es una Familia de Estándares internacionales para Sistemas de Gestión de Seguridad de la Información (SGSI), que propone requerimientos de sistemas de gestión de seguridad de la información, gestión de riesgo, métricas y medidas, guías de implantación, vocabulario y mejora continua.

ISO 27000

En fase de desarrollo. Contendrá términos y definiciones que se emplean en toda la serie 27000. La aplicación de cualquier estándar necesita de un vocabulario claramente definido, que evite distintas interpretaciones de conceptos técnicos y de gestión.

ISO 27001

Es la norma principal de requerimientos del sistema de gestión de seguridad de la información. Tiene su origen en la BS 7799-2:2002 y es la norma con arreglo a la cual serán certificados por auditores externos los SGSI de las organizaciones.

Fue publicada el 15 de Octubre de 2005 y sustituye a la BS 7799-2, habiéndose establecido unas condiciones de transición para aquellas empresas certificadas en esta última.

En su Anexo A, lista en forma de resumen los objetivos de control y controles que desarrolla la ISO17799:2005 (futura ISO27002), para que sean seleccionados por las organizaciones en el desarrollo de sus S GSI; a pesar de no ser obligatoria la implementación de todos los controles enumerados en esta última, la organización deberá argumentar sólidamente la no aplicabilidad de los controles no implementados.

[13] ISO/IEC ISO 27001:2007. (2007). Information Technology- Security Techniques – Information Security Management Systems Requirements Especification. http://iso27000.es

ISO 27002 (ISO 17799)

En fase de desarrollo; probable publicación en 2007. Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. No es certificable. Será la sustituta de la ISO17799:2005, que es la que actualmente está en vigor, y que contiene 39 objetivos de control y 133 controles, agrupados en 11 cláusulas. Como se ha mencionado en su apartado correspondiente, la norma ISO27001 contiene un anexo que resume los controles de ISO17799:2005.

ISO 27003

En fase de desarrollo; probable publicación en Octubre de 2008. Contendrá una guía de implementación de SGSI e información acerca del uso del modelo PDCA y de los requerimientos de sus diferentes fases.

Tiene su origen en el anexo B de la norma BS7799-2 y en la serie de documentos publicados por BSI a lo largo de los años con recomendaciones y guías de implantación.

ISO 27004

Especificará las métricas y las técnicas de medida aplicables para determinar la eficiencia y efectividad de la im plantación de un SGSI y de los controles relacionados. Estas métricas se usan fundamentalmente para la medición de los componentes de la fase “Do” (Implementar y Utilizar) del ciclo PDCA.

ISO 27005

Probable publicación en 2007 ó 2008. Consistirá en una guía para la gestión del riesgo de la seguridad de la información y servirá, por tanto, de apoyo a la ISO27001 y a la implantación de un SGSI. Se basará en la BS7799-3, (publicada en Marzo de 2006) y, probablemente, en ISO 13335.

ISO 27006

Especificará el proceso de acreditación de entidades de certificación y el registro de SGS I.

1.4.3 Beneficios de las Normas ISO 27000.[14]

Entre los beneficios que se obtienen por la implementación del conjunto de normas ISO 27000 en una organización, se tiene:

- Establecimiento de una metodología de gestión de la seguridad clara y estructurada.
- Reducción del riesgo de pérdida, robo o corrupción de información.
- Los clientes tienen acceso a la información a través medidas de seguridad.
- Los riesgos y sus controles son continuamente revisados.
- Confianza de clientes y socios estratégicos por la garantía de calidad y confidencialidad comercial.
- Las auditorías externas ayudan cíclicamente a identificar las debilidades del sistema y las áreas a mejorar.
- El sistema se integra con otros sistemas de gestión (ISO9001, ISO14001, OHSAS).
- Continuidad de las operaciones necesarias de negocio tras incidentes de gravedad.

[14] ISO/EIC 27001:2005. Sistemas de gestión de Seguridad de Información.

- Conformidad con la legislación vigente sobre información personal, propiedad intelectual y otras.

- Imagen de empresa a nivel internacional y elemento diferenciador de la competencia.

- Proporciona confianza y reglas claras a las personas de la organización.

- Reduce costes y mejorar los procesos y servicio.

- Aumenta la motivación y satisfacción del personal.

- Seguridad garantizada en base a la gestión de procesos en vez de en la compra sistemática de productos y tecnologías.

1.4.4 Normativas de Referencia.[15]

Para la aplicación de la norma ISO 27001:2005, es indispensable tener en cuenta la última versión de: "ISO/IEC 17799:2005, Information technology — Security techniques — Code of practice for information security management"

1.5 Términos y Definiciones.[16]

La siguiente terminología aplica a esta norma:

Activo (Asset).

En relación con la seguridad de información, se refiere a cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la organización.

[15] ISO/IEC 17799:2005, Information technology — Security techniques — Code of practice for information security management

[16] Diccionario de la Lengua Española (2007), Vigésima primera edición, Madrid.

Aceptación de Riesgos.

Decisión de aceptar un riesgo

Análisis de Riesgo.-

Uso sistemático de la información para identificar fuentes y estimar el riesgo.

Administración del Riesgo.-

Actividades coordinadas para dirigir y controlar las medidas necesarias para la observación del riesgo dentro de la organización.

Confidencialidad (Confidenciality).-

Acceso a la información por parte únicamente de quienes estén autorizados.

Disponibilidad (Avalaibility).-

Acceso a la información y los sistemas de tratamiento de la misma por parte de los usuarios autorizados cuando lo requieran.

Declaración de Aplicabilidad.-

Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos.

Evaluación de riesgos.-

Proceso de comparar el riesgo estimado contra un criterio de riesgo dado con el objeto de determinar la importancia del riesgo.

Incidente de Seguridad.-

Evento único o serie de eventos de seguridad de la información inesperada o no deseada que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de información.

Integridad.-

Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.

Riesgo Residual.-

El riesgo que permanece tras el tratamiento de riesgos.

Seguridad de la Información.-

Preservación de la confidencialidad, integridad y disponibilidad de la información; además, otras propiedades como autenticidad, responsabilidad, no repudio y fiabilidad pueden ser también consideradas.

Eventos de Seguridad de la Información.-

suceso identificado en un sistema, servicio o estado de la red que indica una posible brecha en la política de seguridad de la información o fallo de las salvaguardias, o una situación anterior o desconocida que podría ser relevante para la seguridad.

Tratamiento de Riesgo.-

Proceso de selección e implementación de medidas para modificar el riesgo.

Valoración de Riesgos.-

Proceso Completo de análisis y evaluación de riesgos.

1.6 Sistema de Gestión de Seguridad de la Información (SGSI).[17]

1.6.1 Antecedentes.

Esta escasa seguridad que hubo en los orígenes del boom de Internet hizo saltar la alarma, de tal forma que la seguridad de la

[17] Areiza, K., Barrientos, A., Rincón, R. y Lalinde, J. (2005); "Hacia un modelo de madurez para la seguridad de la información".

información empezó a tomarse en serio, tanto en el ámbito empresarial, como comercial y por supuesto jurídico-legal. Pero esta seguridad no afecta sólo al tráfico que circula por la red. Debe entenderse la seguridad como algo integral. Debe abordar problemas desde tráfico en red, hasta seguridad física de servidores y bases de datos de información.

Los gerentes de seguridad de la información han esperado mucho tiempo a que alguien tomara el liderazgo para producir un conjunto de normas de seguridad de la información que estuviera sujeto a auditoria y fuera reconocido globalmente. Se cree que un código de normas de la seguridad apoyaría los esfuerzos de los gerentes de tecnología de la información en el sentido que facilitaría la toma de decisión de compra, incrementaría la cooperación entre los múltiples departamentos por ser la seguridad el interés común y ayudaría a consolidar la seguridad como prioridad empresarial.

Desde su publicación por parte de la Organización Internacional de Normas en diciembre de 2000, ISO 17799 surge como la norma técnica de seguridad de la información reconocida a nivel mundial. ISO 17799 se define como "un completo conjunto de controles que incluye las prácticas exitosas de seguridad de la información".

1.6.2 Norma ISO 27001.[18] 14

El SGSI (Sistema de Gestión de Seguridad de la Información) es el concepto sobre el que se construye ISO 27001. La gestión de la seguridad de la información debe realizarse mediante un proceso sistemático, documentado y conocido por toda la organización. Este proceso es el que constituye un SGSI, que podría considerarse, por analogía con una norma tan conocida como la ISO 9001, como el sistema de calidad para la seguridad de la información.

[18] Aguila, A. R, Padilla, A., Serarols, C. y Veciana, J. M. (2005); "La economía digital y su impacto en la empresa: bases teóricas y situación en España". Boletín Económico de Información Comercial Española, n.º 2705, pp. 7-24.

El propósito de un sistema de gestión de la seguridad de la información es, por tanto, garantizar que los riesgos de la seguridad de la información son conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías.

1.6.3 Alcance de la Norma ISO 27001.[19]

ISO/IEC 27001:2005 es una norma que establece los requisitos de los sistemas de gestión de la seguridad de la información. Esta norma está diseñada para asegurar la selección de los controles de seguridad adecuados y proporcionados para proteger la información y dar la confianza a partes interesadas incluyendo a los clientes de una empresa.

Es conveniente para varios tipos diferentes de uso empresarial, incluyendo los siguientes:

- Formulación de exigencias y objetivos para la seguridad.
- Asegurar la gestión más rentable de los riesgos.
- Asegurar el cumplimiento legal.
- Desarrollar un proceso para la puesta en práctica y la gestión de controles para asegurar el conocimiento de los objetivos de seguridad específicos de una empresa.
- Identificación y clarificación de los procesos existentes en la gestión de la seguridad de la información.
- Puede ser usado por la dirección para determinar el estado de las actividades de la gestión de la seguridad de la información.
- Como herramienta de auditores internos y externos para determinar el grado de cumplimiento con la política, directivas y normas adoptadas por una empresa.

[19] Idem.

- Para proporcionar información relevante sobre la política de la seguridad de la información, directivas, normas y procedimientos dentro del mercado.
- Para proporcionar información relevante sobre seguridad de la información a clientes.

1.6.4 Objetivo de la Norma ISO 27001.[20]

Entre los objetivos que se pretenden cumplir con la Norma ISO 27001, tenemos: Aumentar el valor de un servicio "seguro": Esta filosofía supone implementar un SGSI para potenciar un servicio que ya incorpora funciones de seguridad, en el que un SGSI va a aportar beneficios directos.

Potenciar un servicio final: Esta opción supone la implantación de un SGS I ligado a los servicios y/o procesos de negocio. De esta forma, se da un valor añadido a los mismos, bañándolos de una capa de seguridad adicional.

Reforzar los servicios y procesos internos: Esta filosofía pretende implantar el SGSI para fortalecer determinados servicios y procesos internos, en los que una mejora en la seguridad pueda suponer una ventaja para la organización.

En general, se suele traducir en la implementación del SGSI en el área de IT, por ser uno de los principales responsables del tratamiento y conservación de la información de la compañía, o en áreas en las que se maneja información de especial relevancia, como podrían ser las áreas de I+D+i (prototipos, diseños, etc), recursos humanos (datos de carácter personal) o financiero (datos económicos).

[20] De Freitas, V. (2007). La Universidad Simón Bolívar a la luz de los controles de seguridad de la ISO-17799/27001. Ponencia presentada en el IV congreso Iberoamericano de seguridad de la información. Mar del plata. Argentina PP 277-296.

Potenciar la gestión interna: Por último, otra de las filosofías que a veces se utiliza para decidir el alcance es identificar aquellas partes de la organización en las que la implantación del SGSI, como sistema de gestión, sirva para potenciar y estructurar la gestión interna.

Es quizás una de las filosofías más discutibles, ya que existen multitud de sistemas de gestión centrados en distintos aspectos y quizás el de la seguridad pueda no ser el más indicado en todos los casos, pero en determinadas situaciones puede ser una opción.

Ilustración 3. Pirámide de cuatro niveles para la clasificación de documentos

Fuente.: http://www.iso27000.es/sgsi.html

1.6.5 Requisitos de la Documentación del SGSI.[21]

Un Sistema de Gestión de la Seguridad de la Información basado en ISO 27001 está formado por una serie de documentos que pueden clasificarse en una pirámide de cuatro niveles.

[21] Espiñeira, Sheldon y Asociados. Prácticas de Seguridad de Información de las Empresas en Venezuela. Mayo 2008.

La documentación de un SGSI deberá incluir:

Documentos de Nivel 1

Forman el manual de seguridad. Son los siguientes:

Alcance del SGSI: ámbito de la organización que queda sometido al SGS I. Se debe incluir una identificación clara de las dependencias, relaciones y límites que existen entre el alcance y aquellas partes que no hayan sido consideradas, prestando especial atención en aquellos casos en los que el ámbito de influencia del SGSI considere una parte menor de la organización como delegaciones, divisiones, áreas, procesos o tareas concretas.

Política y objetivos de seguridad: documento de contenido genérico que establece el compromiso de la dirección y el enfoque de la organización en la gestión de la seguridad de la información. Metodología de evaluación de riesgos: descripción de cómo se realizará la evaluación de las amenazas, vulnerabilidades, probabilidades de ocurrencia e impactos en relación a los activos de información contenidos dentro del alcance seleccionado.

Informe de evaluación de riesgos: estudio resultante de aplicar la metodología de evaluación anteriormente mencionada. Plan de tratamiento del riesgo: documento que define las acciones para reducir, prevenir, transferir o asumir los riesgos de seguridad de la información e implantar los controles necesarios para proteger la misma.

Declaración de aplicabilidad (SOA -Statement of Applicability-, en sus siglas inglesas): documento que contiene los objetivos de control y los controles contemplados por el SGSI, basado en los resultados de los procesos de evaluación y tratamiento de riesgos, justificando inclusiones y exclusiones.

Procedimientos relativos al nivel 1: procedimientos que regulan cómo se realizan, gestionan y mantienen los documentos enumerados en el nivel 1.

Documentos de Nivel 2

Procedimientos: documentos que aseguran que se realicen de forma eficaz la planificación, operación y control de los procesos de seguridad de la información y describen cómo medir la efectividad de los controles.

Documentos de Nivel 3

Instrucciones, checklists y formularios: documentos que describen cómo se realizan las tareas y las actividades específicas relacionadas con la seguridad de la información.

Documentos de Nivel 4.

Registros: documentos que proporcionan una evidencia objetiva del cumplimiento de los requisitos del SGS I; están asociados a documentos de los otros tres niveles como output que demuestra que se ha cumplido lo indicado en los m ismos.

Control de Documentos

Todos los documentos requeridos por el SGSI serán protegidos y controlados. Un procedimiento documentado deberá establecer las acciones de administración necesarias para:

- Aprobar documentos y prioridades o clasificación de empleo.
- Revisiones, actualizaciones y reaprobaciones de documentos.
- Asegurar que los cambios y las revisiones de documentos sean identificados.
- Asegurar que las últimas versiones de los documentos aplicables estén disponibles y listas para ser usadas.
- Asegurar que los documentos permanezcan legibles y fácilmente

identificables.

- Asegurar que los documentos estén disponibles para quien los necesite y sean transferidos, guardados y finalmente dispuestos acorde a los procedimientos aplicables a su clasificación.
- Asegurar que los documentos de origen externo sean identificados.
- Asegurar el control de la distribución de documentos.
- Prevenir el empleo no deseado de documentos obsoletos y aplicar una clara identificación para poder acceder a ellos y que queden almacenados para cualquier propósito.

1.6.6 Implementación de un SGSI.[22]

Para establecer y gestionar un Sistema de Gestión de la Seguridad de la Información en base a ISO 27001, se utiliza el ciclo continuo PDCA; tradicional en los sistemas de gestión de la calidad.

A continuación se describen los pasos a seguir para la implementación del SGSI:

Plan (Establecer el SGSI)

Definir el alcance del SGSI en términos del negocio. Definir una política de seguridad. Definir una metodología de evaluación del riesgo apropiada para el SGSI y los requerimientos del negocio que especifique los niveles de riesgo aceptables y unos criterios de aceptación de los riesgos.

Identificar y evaluar las distintas opciones de tratamiento de los riesgos Seleccionar los objetivos de control y los controles del Anexo A de la norma ISO 27001 para el tratamiento del riesgo y que cumplan con los requerimientos identificados en el proceso de evaluación y tratamiento del riesgo Definir una declaración de aplicabilidad

[22] Fernández Medina Patón Eduardo, "Seguridad de las Tecnologías de la Información ", Ediciones AENOR (Asociación Española de Normalización y Certificación) España, 2005

Do (Implementar y Utilizar el SGSI)

Definir un plan de tratamiento de riesgos Implantar el plan de tratamiento de riesgos Implementar los controles, definir un sistema de métricas que permita obtener resultados reproducibles y comparables para medir la eficacia de los controles seleccionados.

Procurar programas de formación y concienciación en relación a la seguridad de la información dirigidos a todo el personal. Gestionar las operaciones del SGSI. Gestionar los recursos necesarios asignados al SGSI para el mantenimiento de la seguridad de la información. Implantar procedimientos y controles que permitan una rápida detección y respuesta a los incidentes de seguridad.

Check (Monitorizar y revisar el SGSI)

La organización deberá:

Ejecutar procedimientos de monitorización y revisión Revisar regularmente la efectividad del SGSI. Medir la efectividad de los controles para verificar que se cum ple con los requisitos de seguridad. Revisar regularmente en intervalos planificados las evaluaciones de riesgo, los riesgos residuales y sus niveles aceptables Realizar periódicamente auditorías internas del SGS I en intervalos planificados. Revisar el SGSI por parte de la dirección Actualizar los planes de seguridad Registrar acciones y eventos.

Act (Mantener y mejorar el SGSI)

La organización deberá regularmente:

Implantar en el SGSI las mejoras identificadas. Realizar las acciones preventivas y correctivas adecuadas en relación a la cláusula 8 de la norma ISO 27001. Comunicar las acciones y mejoras a todas las partes interesadas con el nivel de detalle adecuado y acordar, si es pertinente, la forma de proceder. Asegurarse que las mejoras introducidas alcanzan los objetivos previstos.

CAPITULO II.

Datos Generales de la Empresa PCDATA TECHNOLOGIES

CAPITULO II.
DATOS GENERALES DE LA EMPRESA PCDATA TECHNOLOGIES

2.1 Descripción de la Empresa

PCDATA TECHNOLOGIES constituida el 11 de enero del año 2000, conformada por un grupo interdisciplinario de profesionales, que uniendo sus habilidades y conocimientos, se dieron a la tarea de crear empresa. La idea principal, construir una compañía que avance con los adelantos tecnológicos, haciendo del factor humano el bien más preciado.

El portafolio de servicios se inició con InfoContable 1.0 una herramienta pensada para que facilitará a los clientes la obtención y el análisis de la información contable, al día de hoy construyeron herramientas y componentes de software para Integración Inteligente de Información.

2.1.1 Historia y Evolución

Ventures 2000, una oportunidad que aprovechó la empresa para participar en el concurso de planes de negocio. Entre miles de participantes, PCDATA TECNOLOGIES quedó entre los 50 finalistas, lo que llenó de un profundo orgullo y sirvió de plataforma para conocer otras empresas que más adelante serían sus aliados.

Cuenta con la oportunidad de ingresar a la Incubadora de Empresas de Base Tecnológica, quien sería un apoyo para la compañía y un trampolín para avanzar en el tema del crecimiento empresarial. En alianza con Microsoft se realizó el proyecto “CONTROLE SU NEGOCIO”. Este proyecto arrojó muy buenos resultados, gracias al éxito que tuvo InfoContable en las empresas y fue este el inicio de expansión de PCDATA TECNOLOGIES a otras ciudades.

A principios del año 2003 se empezó a comercializar BIABLE (Business Intelligence Avalaible), constituye en una herramienta que posibilita el acceso a la información, dejando de lado las dificultades ocasionadas al momento de extraer información de los sistemas transaccionales.

En el año 2005, el proceso como incubado concluye y por esto decidieron independizarse y crearon una infraestructura propia.

2.2 Gestión Estratégica

2.2.1 Misión

Desarrollo de soluciones tecnológicas innovadoras y del entrenamiento con el que impactan positivamente a los clientes y propiciar el desarrollo del talento humano generando utilidades para las empresas y sus clientes.

2.2.2 Visión

Ser empresa líder, modelo en desarrollo y aplicación de herramientas de tecnología informática; sólida, rentable y en permanente evolución.

2.2.3 Valores Empresariales

- Servicio
- Calidad
- Honestidad
- Compromiso

2.2.4 Principio Corporativo.

- Crecimiento continuo.
- Competitividad.
- Trabajo en equipo.
- Compromiso con el talento humano.
- Democracia participativa.

2.2.5 El Proceso de Desarrollo de Software PCDATA TECNOLOGIES

PCDATA TECNOLOGIES, asegura la creación de productos de software de excelente calidad gracias a su metodología de desarrollo. El más beneficiado con esta metodología es el cliente, quien recibe un producto que satisface y sobrepasa sus necesidades, con altos niveles técnicos y de calidad.

Los principios que rigen el Proceso de Desarrollo de Software son:

- **Tecnología de Objetos.**

PCDATA TECNOLOGIES utiliza las herramientas y metodologías más avanzadas existentes en el medio en Análisis, Diseño, Medición y Programación orientados a Objetos, a fin de poder satisfacer cualquier necesidad del cliente, de tipo técnico o procedimental.

- **Ciclos Evolutivos.**

En PCDATA TECNOLOGIES reconoce que un producto de software nunca está terminado, sino que durante su ciclo de vida deben introducírsele modificaciones permanentemente.

La metodología de desarrollo está diseñada para crear productos por etapas. De esta forma se le permite al cliente introducir nuevas especificaciones durante el proceso de desarrollo, que surgen de la experiencia con el producto, sin estar atado a un contrato inicial que le impida obtener la solución que en realidad necesita.

- **Ensamble y uso de Componentes**

PCDTA TECNOLOGIES garantiza la velocidad y calidad en el desarrollo de software porque para su construcción se utilizan componentes previamente construidos por compañías especializadas, lo cual evita gastar tiempo en construir partes ya que se encuentran prefabricadas. Esto beneficia al cliente porque obtiene su producto en menor tiempo y con mayor calidad.

- **Desarrollo Paralelo**

El Proceso de Desarrollo de Software permite la realización de múltiples tareas modulares de forma paralela, lo que reduce el tiempo de ejecución del proyecto al usar toda la capacidad del equipo de desarrollo. Esto es posible gracias al desarrollo por componentes y la tecnología de desarrollo orientada a objetos.

- **Actividades de Protección**

El Proceso de Desarrollo de PCDTA TECNOLOGIES involucra el desempeño de varias actividades paralelas al desarrollo propiamente dicho. Estas actividades aseguran la calidad del software y la eliminación de desperdicios durante el proceso de desarrollo:

- **Gestión de Configuración del Software (SCM):**

Asegura la correcta administración de la complejidad del Software, la cual aparece al aumentar la cantidad de requisitos y funciones del producto.

- **Control de Versiones (VCS):**

Permite llevar un seguimiento histórico de los cambios hechos al producto e identificar cada versión del producto generada en los ciclos evolutivos del Proceso de Desarrollo de Software.

- **Gestión de Cambios (CM):**

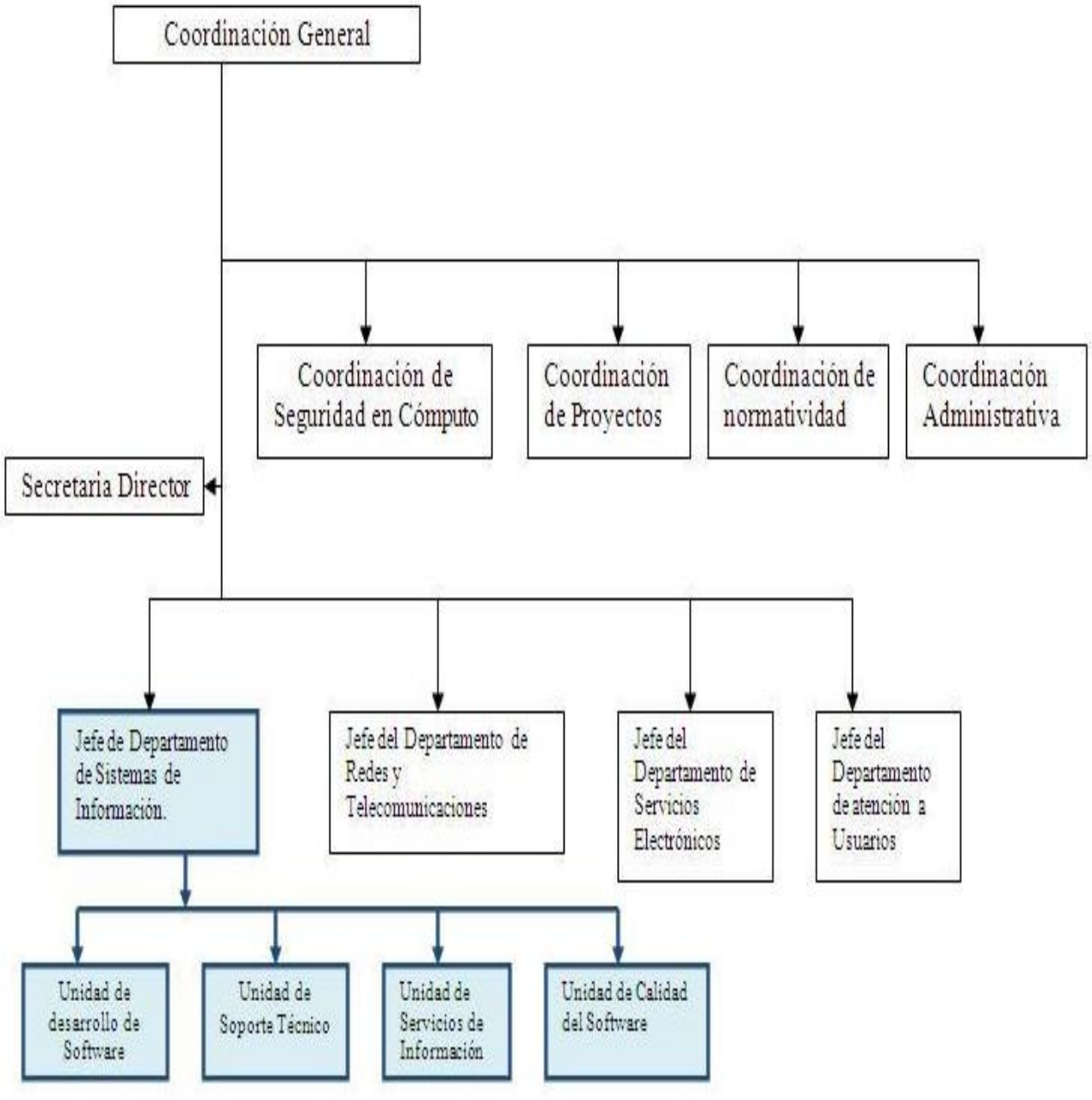
Provee un método formal para identificar, almacenar y aprobar los cambios que deben ser introducidos al producto durante el proceso de desarrollo o en la etapa de mantenimiento del producto.

- **Aseguramiento de Calidad (QA):**

Esta actividad se realiza durante el proceso de desarrollo para garantizar que el producto cumpla las especificaciones del cliente y esté libre de defectos operativos.

2.3 Estructura organizacional

Ilustración 4 Estructura Organizacional



Fuente: Propia Autoría

2.4 Análisis FODA

Tabla No. 1. Análisis FODA.

FACTORES INTERNOS	FACTORES EXTERNOS
Fortalezas	**Oportunidades**
- Motivación de los integrantes del grupo para que se cumpla el proyecto. - Disminución de costos. - Mejoras en los tiempos de atención. - Equipo joven con ideas innovadoras para el desarrollo de actividades y proyectos. - En base a los contactos se obtienen clientes muy fuertes e interesados en nuestro servicio. - Totalmente actualizados con las últimas tecnologías.	- Posibilidad de vender el sistema a otros países. - Alta posibilidad de implementación. - El proyecto es algo innovador y útil a nivel nacional e internacional. - La necesidad de la pequeña y mediana pequeña empresa de implementar tecnologías para el tratamiento de su información. - tecnologías las cuales se pueden implementar en el negocio.
Debilidades	**Amenazas**
- No es posible la dedicación full time al proyecto de parte de los integrantes de grupo. - Reacción negativa a la nueva tecnología de parte de los usuarios. - Problemas de organización en el grupo. - Poca experiencia en la planificación de un proyecto. - Desorientación por sobrecarga de asignaciones. - Por ser un nuevo negocio las demás empresas sienten un grado de desconfianza al momento de optar por nuestros servicios.	- La recesión económica lo que afecta a la empresa en la inversión. - El surgimiento de nuevas competencia. - La inconformidad de los clientes por servicios o productos que no han llenado sus necesidades. - La conformidad de los negocios en seguir utilizando técnicas ordinarias para el tratamiento de la información. - Estrategias mercadológicas de las competencias.

Fuente: Autoría Propia

CAPITULO III.

Propuesta de Implementación de la Norma ISO 27001: 2005 de la Empresa PCDATA TECHNOLOGIES.

CAPITULO III.
PROPUESTA DE IMPLEMENTACION DE LA NORMA ISO 27001:2005 DE LA EMPRESA PCDATA TECHNOLOGIES.

3.1 Metodología de implantación.[23]

La metodología de implantación debe desarrollarse acorde a la cláusulas 4.2 descrita en la Norma ISO 27001:2005 correspondiente al establecimiento y operación de SGSI. La misma que nos indica que debemos definir el alcance y límites del SGSI en términos de las características del negocio, la organización, su ubicación, activos, tecnología e incluyendo los detalles y la justificación de cualquier exclusión del alcance.

La definición del alcance del sistema es responsabilidad de la dirección de la organización bajo el asesoramiento del equipo de trabajo destinado a la gerencia del proyecto. También se acostumbra, para la toma de decisiones coyunturales, constituir un comité de seguridad liderado por el Director o Gerente General y conformado por Gerencias de diferentes áreas como la de tecnología, financiera, Recursos Humanos, Comercial, operaciones, etc.

La cláusula 4.2.1 de la norma también nos indica que debemos establecer una política de seguridad de la información acorde a las características del negocio, organización, activos, regulaciones y tecnología.

Es muy poco exacto redactar una política de seguridad para toda la organización al iniciar el proceso de implantación, la buena práctica es redactarla en paralelo al proceso de acuerdo a las necesidades del sistema, que irán apareciendo. Lo que se recomienda es redactar una Política de Seguridad de Información GENERAL que guíe lo que queremos conseguir mediante nuestro SGSI.

[23] ISO/IEC ISO 17799:2005. (2005). Information Technology- Security Techniques – Information Security Management Systems Requirements Especification. http://17799.com

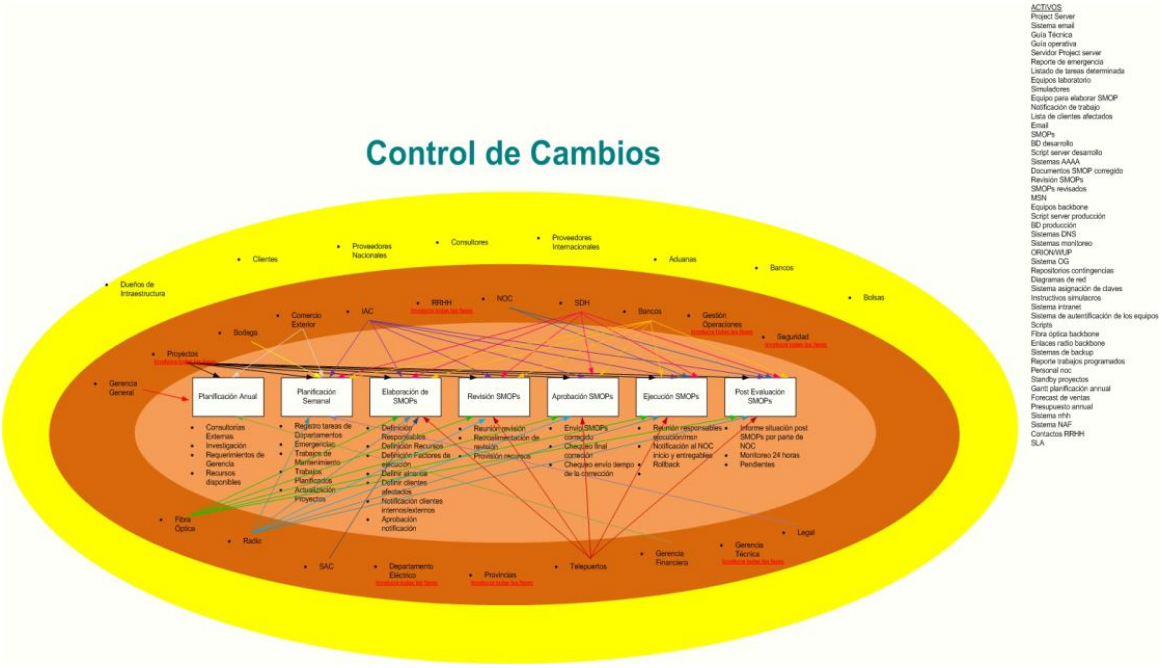
3.1.1 Identificación de los Procesos.[24]

La identificación de procesos dentro del alcance constituye un pilar fundamental para el enfoque del SGSI. Los procesos involucrados son: Monitoreo, Control de cambios, mantenimiento y aprovisionamiento.

3.1.2 Métodos de las elipses

El método de las elipses es un mecanismo que permite identificar dentro de un proceso todas las relaciones de sus subprocesos y actividades con otras áreas de la organización, y entidades externas. Una vez establecidas las relaciones es casi natural poder identificar los activos de información que se usan en dicha relaciones. A continuación se presenta el resultado del método de las elipses para el proceso control de cambios. Este trabajo se lo realiza a manera de un taller interno multidisciplinario para cubrir todas las percepciones.

Ilustración 5 . Método de las elipses.



Fuente: ISO/IEC ISO 27001:2005 (2007). Information technology –security techniques – Information security Management Systems Requirements Specification. Recuperado el 2 de Mayo del 2013 en http://ISO27000.es

[24] Idem

3.1.3 Identificación y tasación de activos

Los activos de información pueden ser el software, el hardware, los enlaces, el equipamiento, los documentos, las personas que manejen (Procesen, trasladen, almacenen) información de valor para el negocio de la organización. El proceso de tasación de activo también es recomendado hacerlo mediante un taller multidisciplinario.

Las relaciones encontradas mediante el método de las elipses nos permitieron visualizar con claridad los activos involucrados. El siguiente paso es tasar el listado de los activos para quedarnos con aquellos de mayor valor. La pregunta para evaluar es ¿la pérdida o deterioro de este activo, cómo afecta la disponibilidad, confidencialidad e integridad del proceso del negocio de la compañía? , en nuestro caso se usó la escala de 1 a 5, siendo el 1 de menor afectación y 5 de mayor afectación.

El valor total del activo es el promedio entero de los valores asignados a la disponibilidad, confidencialidad e integridad. Una vez calculado el valor por cada activo seleccionamos aquellos de mayor valor, el valor umbral queda a discreción de cada organización por ejemplo serán de importancia aquellos con un valor mayor a 3.

3.1.4 Metodologías del análisis y evaluación del riesgo.[25]

De igual manera que en los pasos previos, el análisis y evaluación del riesgo se lo lleva a cabo en un taller multidisciplinario de la organización. Para el análisis y evaluación del riesgo, nos podemos acoger a cualquier metodología conocida. La exigencia de la norma es que dicha metodología arroje resultados comparables y reproducibles, esto quiere decir que el producto debe ser similar si la evaluación la hace otro grupo taller multidisciplinario o si lo hace el grupo taller inicial en otro momento.

[25] Kontio, J. (2006); Empirical Evaluation of a risk management Method, SEI conference on risk management, USA.

La recomendación es usar un método cualitativo para el cálculo del riesgo, puesto que puede abarcar todos los activos con mayor facilidad. El método cuantitativo exigiría que todo sea llevado a valor monetario y en la mayoría de los casos esta tarea es complicada y/o tarda demasiado, puesto que no sólo implica el valor comercial de los activos sino también de la afectación que pueden tener su entorno.

La metodología consiste que para cada activo identificar todas las amenazas existentes, la posibilidad de ocurrencia de estas amenazas, las vulnerabilidades que pueden hacer que dicha amenaza se materialice y la posibilidad que dicha amenaza penetre tal vulnerabilidad. El valor del riesgo está dado por el producto matemático del valor del activo, encontrado en la tasación, por el valor de la mayor de posibilidad de amenaza. La escala para calcular las posibilidades es de 1 al 5, siendo 5 mayor. De la misma forma como en la tasación de activos se puede descartar las de menor valor para enfocarnos en las verdaderamente importantes, el valor del umbral es decisión del grupo taller.

3.1.5 Tratamiento del riesgo.[26]

El análisis y evaluación riesgo permitió valorizar el riesgo y conocer cuáles son los activos de información que tienen mayor exposición por lo tanto saber a dónde enfocar los recursos de la organización.

El riesgo tiene 4 opciones de tratamiento que son:

- Reducir el riesgo, con la aplicación de contramedidas o salvaguardas especificadas controles del Anexo A de la norma.
- Evitar el riesgo, dejando de realizar la actividad que produce el riesgo.
- Transferir el riesgo, a un tercero como por ejemplo una aseguradora o una tercerización de servicios.

[26] King, A.A., Lenox, M.J. y Terlaak, A.K. (2005). "The strategic use of decentralized institutions: Exploring certification with the ISO 27001 management standard", Academy of Management Journal, Vol. 48, núm. 6.

- Aceptar el riego, que consiste en asumir la responsabilidad de correr dicho riesgo.

La opción de aceptación de un riesgo deber ser aprobada formalmente por la dirección de la compañía, en la mayoría de casos se presenta esta situación cuando el control necesario de implantar tiene un valor económico mayor que el mismo activo.

3.1.6 Selección de controles.[27]

Los controles son las contramedidas o salvaguardas especificadas en el Anexo A de la Norma ISO 27001:2005, enfocados a los 11 dominios de cobertura de la norma, como son:

- A.5 Política de seguridad.
- A.6 Organización de la seguridad de la información.
- A.7 Gestión de activos.
- A.8 Seguridad de los recursos humanos.
- A.9 Seguridad física y ambiental.
- A.10 Gestión de las comunicaciones y operaciones.
- A.11 Control de acceso.
- A.12 Adquisición, desarrollo y mantenimiento de los sistemas de información.
- A.13 Gestión de incidentes en seguridad de la información.
- A.14 Gestión de la continuidad del negocio.
- A.15 Cumplimiento.

La selección de los controles que la organización debe implementar se lo hace por 3 fuentes:

- Del tratamiento del riesgo, orientados a eliminar vulnerabilidades o minimizar el impactos.
- Los requerimientos legales (implementación no es discutible).

[27] Idem

- Producto de las operaciones en el negocio de la compañía.

Si se requiere una mayor ampliación de las prácticas para implementar los controles se puede referenciar a la ISO 17799:2005. También existe la posibilidad de que la organización cree sus propios controles puesto que los que se describen en la norma no se adapta a nuestras necesidades. En nuestro caso creamos un control con la nomenclatura T1 que se refiere a tener un equipo de contingencia.

3.1.7 Medición de efectividad de los controles.[28]

Una vez que los controles han sido implantados es necesario revisarlos constantemente que estén cumpliendo su objetivo. La medición de los controles se lo puede hacer mediante indicadores de efectividad, por ejemplo, si luego del análisis y evaluación de riesgo sobre el activo "Nodos Edge", salta a la luz que debemos implementar u optimizar el control A.9.2.2 de la Norma ISO 27001:2005 (Anexo A) cuyo objetivo de control son los servicios público que indicaron que los equipos deben ser protegido de fallas de energía y otras interrupciones por fallas de los servicios públicos.

Los indicadores pueden ser de tipo seguimiento o de rendimiento, un indicador de seguimiento aplicado al control A.9.2.2 es el porcentaje de "Nodos Edges" por cada ciudad que pierde conectividad durante un apagón nacional.

Un indicador de rendimiento o performance puede ser el Tiempo de Supervivencia Real de un Nodo Edge durante un apagón / sobre el Tiempo estimado de respaldo, este indicador mostraría que tan acertados han sido los trabajos de mantenimiento. El indicador más significativo para un proveedor de servicio de telecomunicaciones es el llamado Acuerdo de Nivel de Servicios o SLA (*Service Level Agreement) por sus siglas en inglés,* establecido en los contratos, medido en porcentaje de disponibilidad del servicio. En términos

[28] O'hehir, M. (2006); What is Business Continuity Planning Strategy?, en Business Continuity Management, Wiley, Londres.

generales consiste en calcular el tiempo de disponibilidad de un enlace dividido sobre el tiempo transcurrido. En implementaciones más sofisticadas el SLA también se puede ver afectado por variables o sub-indicadores como son el porcentaje de paquetes perdidos, jitter y/o delays.

Cada organización debe escoger los indicadores que económica y operativamente sean factibles implementar y llevar a cabo su medición. Pero sobre todas las cosas estas mediciones deben agregar valor a los objetivos del negocio de la compañía.

Algunos indicadores de tecnología son: porcentaje de falsos positivos de un IDS/IPS, porcentaje de disponibilidad de un Servidor WEB, porcentaje de solución de Incidentes que se extiende más de un tiempo X, Número de casos de Phishing presentados en el mes por ciudad, Número de Clientes que caen en listas negras de SPAM por Ciudad, Número de empleados infectados con virus por mes por ciudad.

3.1.8 Requisitos documentales

En toda implementación de sistemas de gestión, un factor a superar es el sistema documental exigidos por la norma, entre los principales motivos podemos mencionar:

- Se percibe como una carga operativa que no se quiere asumir.
- Rechazo al cambio.
- Informalidad muy institucionalizada.

Para poder obtener una certificación, hay que superarlo y utilizar mecanismos tecnológicos que faciliten la institucionalización del sistema documental. La recomendación es implementar un sistema intranet que pudiera usar protocolo HTTP y/o FTP para la gestión de documentos. Dicho sistema debe manejar perfiles y roles así como también características del modelo AAA

(Authentication, Authorization, Accounting). La ISO 27001 tiene exigencias documentales que se indican en la cláusula 4.3 de dicha norma y son: 23

- Enunciado de la política de seguridad y los objetivos.
- El alcance del SGSI.
- Procedimientos y controles de soporte del SGSI.
- Una descripción de la metodología de evaluación del riesgo.
- Reporte de la evaluación del riesgo.
- Plan de tratamiento del riesgo.
- Enunciado o declaración de aplicabilidad.
- Procedimientos documentados necesarios por la organización para asegurar la planeación, operación y control de sus procesos de seguridad de la información y describir cómo medir la efectividad de los controles.
- Registros requeridos por este estándar internacional.

Los procedimientos documentados son:

- Debe existir un procedimiento documentados que especifique el manejo de documentos como es la creación, nomenclatura, aprobación, obsolescencia, cambios, etc.
- Debe existir un procedimiento documentado para el manejo de las auditorías, reporte de resultados y mantenimiento de registros.
- Debe existir un procedimiento documentado para el manejo de acciones correctivas.
- Debe existir un procedimiento documentado para el manejo de acciones preventivas.

Se deben mantener registros de:

- Auditorías realizadas.
- Resultados de las revisiones por la gerencia.
- Registros de capacitación, competencias, capacidades, experiencias y calificaciones.

- Y todos aquellos registros que otorguen evidencia objetiva del cumplimiento con la norma.

Una buena práctica es identificar textualmente todos los “debes” dentro de la redacción de la norma para así poder identificar las exigencias explícitas.

3.1.9 Factores de éxito

Existen factores que son claves para una implantación exitosa del sistema de gestión de seguridad de la información. Entre ellos podemos mencionar:

- Compromiso de la dirección con el SGSI.
- Objetivos del SGSI deben estar alineados con el negocio de la compañía.
- Liderazgo de la gerencia del proyecto.
- Motivación del personal.
- Concientización de toda la organización para con la seguridad.
- Embeber en todos los procesos del negocio el ciclo PLAN-DO-CHECKACT
- Establecer claramente las responsabilidades y obligaciones de cada persona dentro del SGSI.

3.2 Certificación ISO 27001:2005.[29]

Una vez que se ha cumplido el ciclo PLAN-DO-CHECK-ACT del SGSI bajo todos los exigibles de la Norma ISO 27001:2005. Podemos optar por una certificación formal de nuestro sistema, para ello es necesario contratar los servicios de una empresa certificadora autorizada.

3.2.1 Proceso de certificación.[30]

El proceso de certificación empieza con la elección de la empresa certificadora, en nuestro medio es posible contar con tres compañías: BSI, BVQI, SGS. A la empresa certificadora se le entrega información que les permita

[29] Pradas, J. (2005); “El sector digital como facilitador del cambio económico y de la naturaleza de la empresa”, Economía Industrial, n.º 325, pp. 83-102.
[30] Idem.

estimar la duración de las fases de certificación, como puede ser: el alcance número de empleados en el SGSI, cantidad de activos, ubicaciones geográficas, si ya cuenta con otro sistema de gestión (ej. ISO 9001). Algunas organizaciones optan por contratar una pre-auditoria con el fin de diagnóstico, antes de contratar la auditoría formal.

La certificación del SGSI bajo la norma ISO 27001:2005 consta de dos fases:

FASE I: Aquí se verifica el cumplimiento documental del sistema y se puede detectar fallas medulares en la implementación. En esta fase el Auditor Externo debe emitir un informe favorable para continuar o no con la Auditoría de FASE II. Por lo general entre FASE I y FASE II no pude exceder más de 30 días, pero es el cliente quien propone las fechas exactas para llevar a cabo cada una de las FASES de la Auditoría.

FASE II: El objetivo de esta fase, es que la certificadora verifique objetivamente la implantación correcta del SGSI bajo todas las exigencias de la norma. El equipo de auditores mediante muestreo verificará el cumplimiento de todas o la mayoría de áreas dentro del alcance del SGSI.

Como auditado es necesario mantener a la mano todos los procedimientos, registros, formatos y acceso a sistemas que sirvan como evidencia del cumplimiento.

El último día de la auditoría se lleva a cabo la reunión de cierre donde el Auditor Líder presenta el informe donde se especifica los hallazgos y se recomienda o no para la certificación.

Si el informe es favorable, la empresa certificadora debe enviar a la Empresa Acreditara quien es la que emite el certificado una vez que aprueba el informe.

3.2.2 Auditorías internas.[31]

Las auditorías internas es el proceso interno de revisión del SGSI en conformidad con la NORMA ISO 27001:2005. La premisa de todas las auditorías, por consiguiente de todo auditor, es buscar conformidades más no no-conformidades. La ISO 27001:2005 exigen que la organización haya llevado a cabo auditorías internas y los resultados de las mismas sean revisados por la dirección. Por lo general las auditorías internas se las lleva a cabo antes de la auditoría externa y esta última se recomienda mínimo una vez al año.

Mientras más exigente y formales sean las auditorías internas mayor valor agregarán a la preparación de la organización. Estas auditorías pueden ser ejecutadas por personal interno de la compañía con formación como auditores internos o en su defecto puede ser llevado a cabo por personal externo como ejemplo una empresa consultora. Lo recomendación es que sea personal interno quien realice las auditoría de una forma cruzada entre los diferente áreas de la organización, o sea que nadie puede auditar su propia área.

Las organizaciones deben manejar programas de auditoría (cronograma general o anual), planes de auditorías (objetivos, horarios y secuencia de auditorías) y listas de chequeo (preguntas puntuales por área). Son herramientas que ayudan a las planificar, ejecutar y reportar las auditorías internas. Dentro del informe de auditoría se debe especificar las conformidades generales o fortalezas, no conformidades, observaciones y oportunidades de mejora. La definición de cada una de ellos es la siguiente:

Las **no conformidades** son aquellas oposiciones a la norma que se pueden redactar con el lenguaje natural de la misma. Es decir contrario a todos los DEBES textuales de la redacción.

[31] Velásquez, N. y Estayno, M. (2007); "Desarrollo y Mantenimiento Seguro de Software para Pymes: MoProSoft alineado a ISO/IEC 17799:2005", IV Congreso Iberoamericano de Seguridad Informática, Mar de Plata. Argentina. Pp. 101-110.

Las **observaciones** son situaciones que a pesar de no ser no-conformidades pueden transformarse en ellas, sino se les da el tratamiento debido.

Las **oportunidades de mejora** son los puntos en que se puede sofisticar el sistema.

3.2.3 Auditorías de Terceras partes.[32]

Las auditorías de terceras parte dentro del contexto refieren a las auditorías externas que pueden ser llevadas a cabo por una entidad certificadora, empresa consultora, clientes.

Cada uno con sus fines específicos. Dependiendo del tamaño de la organización la auditoría externa puede ser llevada a cabo por un equipo de auditores dirigidos por un auditor líder. Es responsabilidad de la empresa certificadora enviar el plan de auditoría especificando los horarios por área a ser auditada.

La empresa auditada debe prever disponibilidad de un representante del área para ser auditado en el horario establecido, pero esto no impide que el auditor entreviste a cualquier miembro del departamento consultándole aspectos generales y fundamentales como son la política general, los objetivos del SGSI de la empresa o el procedimiento para reportar incidentes.

La auditoría externa inicia con una reunión de apertura con los directivos de la organización, aquí se validará el alcance de la auditoría y se expondrá cualquier inconveniente logístico de último momento. Al final de cada día es buena práctica, por el auditor, exponer los hallazgos para que la directiva de la organización esté consciente del avance de la auditoría.

[32] Hiles, A. (2005) Business Continuity Best Practices. Rothsein Associates.Inc.

Al final del último día el auditor líder expondrá el informe de auditoría donde se incluirán todos los hallazgos encontrados, conformidades o fortalezas a resaltar, no-conformidades mayores, no-conformidades menores, observaciones y oportunidades de mejora. Dicho informe será enviado a la empresa certificadora y de ser favorable al organismo acreditador.

La organización debe evitar a toda costa las no-conformidades MAYORES, puesto que la presencia de una de ellas es un impedimento de recomendación de certificación. Se identifican como **NO-CONFORMIDADES MAYORES**, cuando se presentan las siguientes situaciones:

- No cumplimiento de la norma ISO 27001:2005 que afecte el núcleo del SGSI en cualquier punto del ciclo PLAN-DO-CHECK-ACT. Es decir una situación que puede afectar las bases del SGSI y por ende todo su funcionamiento.
- La múltiple repetición de una misma no-conformidad menor en muchas áreas de la organización también produce una MAYOR.
- Un área de la organización con muchas no-conformidades menores también produce una no-conformidad MAYOR.
- Desde el rol de auditor la premisa es que si se duda que una no-conformidad es mayor o menor entonces es menor.
- Algunas no conformidades mayores son: la metodología errónea para el análisis y evaluación de riesgo, no haber hecho auditorías internas, no existir la revisión por la dirección.

3.3 Recursos necesarios.[33]

Esta norma está pensada para que cualquier empresa pueda implementarla independientemente el poder económico que ella posea.

[33] Stoneburner, G., Goguen, A. y Feringa, A. (2006); Recommendations of the National Institute of Standards and Technology, University of the Aegean, Karlovasi Greece. July.

En realidad, una mayor cantidad de recursos económicos, pueden ser diferenciadores en lo que respecta a la cantidad de tareas automatizadas que se pueden adoptar, por consiguiente la carga operativa en planear, implementar, monitorear y mejorar el SGSI es menor y más llevadero para toda la organización, a diferencia de procedimientos manuales y documentos impresos.

3.3.1 Puntos claves de Inversión.[34]

Se recomienda que la organización enfoque la inversión en los siguientes puntos:

- Capacitación del personal clave: manager del proyecto, miembros del equipo de trabajo.
- Mecanismos de concientización de todo el personal.
- Formación de un equipo de auditores internos.
- Formación de Auditor Líder certificado ISO 27001:2005 por IRCA.
- Pre-auditoría de diagnóstico.
- Automatización y/o elaboración de herramientas de apoyen la medición de los controles, mejoramiento continuo.
- Crear un ambiente favorable en los talleres multidisciplinario.

3.3.2 Retorno de Inversión.[35]

El cálculo de retorno de inversión (ROI) siempre ha sido una herramienta muy adecuada para justificar inversiones de cara a la gerencia de una organización. Ver beneficios no siempre es fácil, por eso este tipo de cálculos han ido ganando protagonismo en los últimos tiempos. En el caso particular de inversiones en seguridad, el término a utilizar se denomina ROSI (Return Of Security Investment) y al igual que ROI mide la relación entre el retorno que produce una inversión y la inversión propiamente dicha.

---

[34] Idem.
[35] Alexander Alberto Ph.D , Diseño de un Sistema de Gestión de Seguridad, Editorial Alfaomega, Colombia, 2007

Centrándonos en ROSI, la esencia del cálculo se basa en calcular los costes ahorrados como consecuencia de evitar incidentes de seguridad o de mitigar los efectos de los mismos en caso de ocurrencia. Es por esto que en ROSI el beneficio es en realidad el ahorro conseguido (además de otro tipo de beneficios como pueden ser mejorar la imagen de la empresa consiguiendo así nuevos clientes).

ISO 27001 nos aporta confianza en este sentido, ya que habiendo implantado un sistema de gestión en seguridad de la información (SGSI) como se define en dicho estándar nos estamos asegurando una importante reducción y eliminación de incidentes de seguridad.

Además, al estar dentro de un ciclo de mejora continua, conseguimos que el sistema de gestión responda a las nuevas necesidades de seguridad de la organización que vayan apareciendo.

A través de los diferentes controles de seguridad que plantea ISO 27001 en su ANEXO A podemos reducir de forma considerable la gran mayoría de incidentes que en caso de no implantar ningún sistema de seguridad podrían amenazar nuestra organización.

Otro factor clave a la hora de calcular el retorno de inversión en proyectos de implantación ISO 27001 es el hecho de tener que contar con un Plan de Continuidad de Negocio (BCP, Business Continuity Plan). Gracias a un BCP tendremos asegurada –en un alto porcentaje- la continuidad de nuestro negocio en caso de desastre, como por ejemplo un incendio o un terremoto. Si bien en estos casos vamos a sufrir un importante daño en cuanto a costos, el hecho de poder seguir prestando servicios a nuestros clientes nos reporta unos beneficios que están muy por encima de los costos en implantar el plan (y nos evita las pérdidas de no poder prestar servicio, además de evitar daño hacia la imagen de nuestra marca y la percepción negativa que se llevaría el cliente).

3.3.3 ROSI e ISO 27001. Integración.[36]

La norma ISO 27001 contempla en todas sus fases elementos que son perfectamente integrables dentro de un estudio de retorno de inversión en seguridad.

- **Inventario y valoración de activos:** en esta etapa evaluamos el valor que para la organización tiene cada uno de los activos a incluir dentro del alcance del SGSI a implantar.

- **Análisis de riesgos sobre los activos:** se estudia las amenazas que podrían materializarse sobre los activos y los procesos de negocio.

- **Tratamiento de esos riesgos (reducción de incidentes):** en esta fase es donde se implantan los controles de seguridad que harán reducir o eliminar los incidentes de seguridad. Posteriormente se medirá la eficacia de esos controles para comprobar que realmente están siendo útiles para proteger la organización.

- **Plan de continuidad (BCP):** un plan de continuidad de negocio, como su propio nombre indica, asegura poder seguir dando servicio a los clientes en caso de catástrofes de origen natural (terremotos, inundaciones, etc.), industrial (incendios, explosiones, averías, etc.) o humano (errores no intencionados, ataques deliberados). Si bien implantar un BCP es costoso en tiempo y dinero, los beneficios obtenidos en caso de ocurrir un incidente grave pueden ser incalculables.

- **Mejora continua:** ISO 27001 contempla en su cláusula 8 la mejora continua del sistema, basada en mejorar la eficacia del SGSI implantado y responder a las nuevas necesidades en seguridad de la información que

[36] Alexander Alberto Ph.D , Diseño de un Sistema de Gestión de Seguridad, Editorial Alfaomega, Colombia, 2007

tiene la empresa. Para enlazar este punto con el cálculo del ROSI podemos pensar que un sistema de seguridad que no se mantenga "vivo" en el tiempo no podrá responder con las garantías oportunas ante las nuevas incidencias de seguridad que podrían afectar a el negocio.

3.3.4 Estimación del Retorno de la Inversión.[37],[38]

Tabla No. 2. Sumario de Valores del Análisis ROSI

SUMARIO DE VALORES DEL ANALISIS ROSI	
Pérdidas Anuales por Incidentes - Sin tratar	$ 1,440,000
Pérdidas Anuales por Incidentes - Residual luego de mitigados	$ 671,000
Ahorro Bruto Anual por Contramedidas	$ 769,000
Costo Inicial Contramedidas	$ 278,000
Costos Anuales Recurrentes Contramedidas	$ 82,000

CALCULO DE ROSI (valores en miles)					
Años		**0**	**1**	**2**	**3**
Ahorro Bruto Anual			$ 769	$ 769	$ 769
Ahorro Bruto Anual a valor actual dto. 15%			$ 669	$ 581	$ 506
Valor Contramedidas	$ 1,756				
Costos Contramedidas		$ 278	$ 82	$ 82	$ 82
Costos Contramedidas a valor actual dto. 15%		$ 278	$ 71	$ 62	$ 54
Costo Contramedidas	$ 465				
Retorno (Valor - Costo)	$ 1,291				
ROSI (Retorno/Costo)	277 %	Igual a un:	56 %	anual	

Fuente: Caso práctico obtenido en "ROSI, el ROI de la Seguridad de la Información" por Carlos Ormella Meyer. Abril de 2006

Una fórmula sencilla para el cálculo del ROSI podría ser la siguiente:

ROSI = [(BENEFICIO – COSTOS) / COSTOS] * 100%

[37] Caso práctico obtenido en "rosi, el roi de la seguridad de la, información" por carlos ormella meyer. Abril de 2006.

[38] Caso práctico obtenido en "calculating security return on investment". Don o'neill, software engineering institute. Carnegie mellon university. 2007

Savings: = (Resistance Savings + Recognition Savings + Reconstitution Savings)

Cost: = (Total Preparation + Total Cleanup + Total Lost Opportunity + Total Critical

Infrastructure Impact)

Where: Incidents: = 100 [Expected number of incidents]

IR1: Number of expected incidents successfully resisted = 60

IR2: Number of expected incidents successfully recognized = 30

IR3: Number of expected incidents successfully survived = 5

IR4: Number of expected incidents undetected (duds) except for a forensic trace = 5

Resistance Savings

SR1: = IR1 * (Cleanup1 + Lost Opportunity1 + Critical Infrastructure Impact1)

SR1: = 60 * (2,500 + 10,000 + 0) = 750,000

Recognition Savings

SR2: = IR2 * (Cleanup2 + Lost Opportunity2 + Critical Infrastructure Impact2)

SR2: = 30 * (25,000 + 20,000 + 0) = 1,350,000

Reconstitution Savings

SR3: = IR3 * (Cleanup3 + Lost Opportunity3 + Critical Infrastructure Impact3)

SR3: = 5 * (250,000 + 500,000 +5,000,000) = 28,750,000

Dud Costs

SR4: = IR4 * (Cleanup4)

SR4: = 5 * (250) = 1,250

Preparation

Step 1: = 75,000 [3 days * 50 participants * $500/day]

Step 2: = 75,000 [5 days * 25 participants * $600/day]

Step 3: = 250,000 [Resistance and Recognition implementation costs]

Step 4: = 500,000 [Reconstitution implementation costs]

Step 5: = 50,000 [Information disclosure control costs]

Total Preparation: = (Step1 + Step2 + Step3 + Step4 + Step5)

Total Preparation: = (75,000 + 75,000+ 250,000 + 500,000 + 50,000)

Total Preparation: = 950,000

Cleanup Per Incident

Cleanup1: = [2,500/incident]

Cleanup2: = [25,000/incident]

Cleanup3: = [250,000/incident]

Cleanup4: = [250/incident]

Total Cleanup: = (IR1 * Cleanup1) + (IR2 * Cleanup2) + (IR3 * Cleanup3) + (IR4 * Cleanup4)

Total Cleanup: = (60 * 2,500) + (30 * 25,000) + (5* 250,000) + (5 * 250) = 150,000 + 750,000 + 1,250,000 + 1,250

Total Cleanup: = 2,151,250

Lost Opportunity Per Incident

Lost Opportunity1:= 0.1 day * 10,000/day: = 10,000

Lost Opportunity2:= 0.2 days * 10,000/day: = 20,000

Lost Opportunity3:= 5 days * 100,000/day:= 500,000

Total Lost Opportunity: = (IR1 * Lost Opportunity1) + (IR2 * Lost Opportunity2) + (IR3 *

Lost Opportunity3)

Total Lost Opportunity: = (60 * 10,000) + (30 * 20,000) + (5 *500,000)

Total Opportunity: = 600,000 + 600,000 + 2,500,000

Total Lost Opportunity: = 3,700,000

Critical Infrastructure Impact Per Incident

Critical Infrastructure Impact1:= 0 * 1,000,000:= 0

Critical Infrastructure Impact2:= 0 * 1,000,000:= 0

Critical Infrastructure Impact3:= 5 * 1,000,000:= 5,000,000

Total Critical Infrastructure Impact: = (60 * 0) + (30 * 0) + (5* 5,000,000): = 25,000,000

Savings: = (Resistance Savings + Recognition Savings + Reconstitution Savings)

Cost: = (Total Preparation + Total Cleanup + Total Lost Opportunity + Total Critical Infrastructure Impact)

Savings: = 750,000 + 1,350,000 + 28,750,000) = 30,850,000

Cost: = (950,000 + 2,151,250 + 3,700,000 + 25,000,000) = 31,801,250

ROI: = Savings/Cost

ROI: = 30,850,000/31,801,250

ROI: = 0.97008765379

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES Y RECOMENDACIONES

1. La norma ISO 27001:2005 está orientada al tratamiento de la seguridad de la información mediante la gestión del riesgo, tanto para sus activos como para sus procesos. Esto garantiza que ante recursos limitados las inversiones sean bien focalizadas.

2. Hay decisiones respecto al cumplimiento de políticas dentro SGSI que deben ser de carácter jerárquico, impulsado por el director de la organización, siendo este el primer paso para adaptarse a todo cambio coyuntural dentro de la empresa.

3. Para poder tener una implantación exitosa del SGSI, los objetivos del mismo deben estar alineados al negocio de la compañía, caso contrario el valor que agrega no sería muy tangible.

4. La concientización de la compañía es un pilar fundamental de esta norma, por lo cual las organizaciones deben ingeniosamente buscar y adoptar mecanismos que permitan que se despierte un interés y compromiso por parte de todos los empleados.

   Existen mecanismos como bonos, viajes, cenas o reconocimientos públicos que siempre despiertan interés.

5. Las organizaciones deben tratar de hacer lo más llevadero posible las tareas operativas del sistema SGSI, para lo cual necesitan la ayuda de herramientas tecnológicas que automaticen ciertas tareas.

6. Contar con personal clave dentro de la empresa y con las competencias exigidas por la Norma ISO 27001:2005 evitan la contratación de consultorías externas cuyo costo suele ser alto.

7. Un SGSI no puede ser implantado por moda sino siempre buscando objetivos claros que agreguen valor a la organización. Toda nueva implementación en pro de mejoras en la seguridad de la información debe ir acompañado de políticas funcionales que direccionen los esfuerzos hacia los objetivos del SGSI.

8. El tener implantado un SGSI certificado bajo la norma ISO 27001:2005 no significar contar con seguridad máxima en la información de la organización sino que esto significa que la empresa cumple con los requerimientos y mejores prácticas establecidas en dicha norma para que su SGSI actual funcione correctamente y además pueda evolucionar hacia la sofisticación.

9. El eslabón más débil de la cadena son las personas, por lo tanto dentro del análisis y evaluación del riesgo del SGSI se debe dar el énfasis necesario para considerar este tipo de amenazas. Siempre aplicando en los perfiles el principio del mínimo conocimiento.

REFERENCIAS BIBLIOGRAFICAS

REFERENCIA BIBLIOGRAFICAS

- Albts, C. y Dorofee, A. (2005). Managing Information Security Risk. Pearson Education.
- Alexander, A. (2007). Diseño de un sistema de gestión de seguridad de información. Alfaomega.
- Aceituno, V. (2006); Information Security Management Maturity Model. ISM3. ISECOM.
- Aguila, A. R, Padilla, A., Serarols, C. y Veciana, J. M. (2005); "La economía digital y su impacto en la empresa: bases teóricas y situación en España". Boletín Económico de Información Comercial Española, n.º 2705, pp. 7-24.
- Areiza, K., Barrientos, A., Rincón, R. y Lalinde, J. (2005); "Hacia un modelo de madurez para la seguridad de la información", Memorias del Congreso Iberoamericano de Seguridad Informática, Valparaíso. Argentina.
- Alexander Alberto Ph.D , Diseño de un Sistema de Gestión de Seguridad
- Editorial Alfaomega, Colombia, 2007
- Barnes, J. (2005). A Guide to Business Continuity Planning. Wiley.London
- British Standard Institute , Website www.bsi.com
- CASO PRÁCTICO OBTENIDO EN "ROSI, EL ROI DE LA SEGURIDAD DE LA
- INFORMACIÓN" por Carlos Ormella Meyer. Abril de 2006.
- CASO PRÁCTICO OBTENIDO EN "Calculating Security Return on Investment". Don O'Neill, Software Engineering Institute. Carnegie Mellon University. 2007
- De Freitas, V. (2007). La Universidad Simón Bolívar a la luz de los controles de seguridad de la ISO-17799/27001. Ponencia presentada en el IV congreso Iberoamericano de seguridad de la información. Mar del plata. Argentina PP 277-296.
- Diccionario de la Lengua Española (2007), Vigésima primera edición, Madrid.
- Espiñeira, Sheldon y Asociados. Prácticas de Seguridad de Información de las Empresas en Venezuela. Mayo 2008. http://pwc.com
- Fernández Medina Patón Eduardo, "Seguridad de las Tecnologías de la Información ", Ediciones AENOR (Asociación Española de Normalización y Certificación) España, 2005
- "Gestión del riesgo: Principios de implementación de herramientas y métodos

- para la evaluación y gestión del riesgo para inventarios", Agencia de Redes y
- Seguridad de la Información de la Unión Europea (ENISA), 2006
- Hiles, A. (2005) Business Continuity Best Practices. Rothsein Associates. Inc.
- Hoffman, T. (2006); "Risk management still a wild frontier", Computerworld, 32(7), p. 10.
- International Standard Organization, Norma ISO/IEC FDIS 27001:2005(E).
- ISO/IEC guide 73:2006. Risk Management – Vocabulary – Guidelines for use in standards.
- ISO/IEC ISO 17799:2005. (2005). Information Technology- Security Techniques – Information Security Management Systems Requirements Especification. http://17799.com
- ISO/IEC ISO 27001:2007. (2007). Information Technology- Security Techniques – Information Security Management Systems Requirements Especification. http://iso27000.es
- ISO/EIC 27001:2005. Sistemas de gestión de Seguridad de Información.
- Kontio, J. (2006); Empirical Evaluation of a risk management Method, SEI conference on risk management, USA.
- King, A.A., Lenox, M.J. y Terlaak, A.K. (2005). "The strategic use of decentralized institutions: Exploring certification with the ISO 27001 management standard", Academy of Management Journal, Vol. 48, núm. 6.
- O'hehir, M. (2006); What is Business Continuity Planning Strategy?, en Business Continuity Management, Wiley, Londres.
- Peltier, T. (2005); Information Security Risk Analysis, Auerbach, London.
- Pradas, J. (2005); "El sector digital como facilitador del cambio económico y de la naturaleza de la empresa", Economía Industrial, n.º 325, pp. 83-102.
- Sheffi, Y. (2005); The Resilient Enterprise, MIT Press, Boston.
- Stoneburner, G., Goguen, A. y Feringa, A. (2006); Recommendations of the National Institute of Standards and Technology, University of the Aegean, Karlovasi Greece. July.
- Velásquez, N. y Estayno, M. (2007); "Desarrollo y Mantenimiento Seguro de Software para Pymes: MoProSoft alineado a ISO/IEC 17799:2005", IV Congreso Iberoamericano de Seguridad Informática, Mar de Plata. Argentina. Pp. 101-110.

ANEXOS

Escuela de Graduados

Trabajo Final de Investigación para Optar por el Título de:

Maestría en Gerencia y Productividad

Propuesta de Implementación de la Norma ISO 27001:2005 Grupo PCDATA TECHNOLOGIES en la Ciudad de Santo Domingo 2013

Sustentante:

Pedro M. Castillo R. **2011-0670**

Asesor (a):

Edda Freites Mejia, MBA

Santo Domingo, Rep. Dom.
Agosto, 2013

I. TITULO

PROPUESTA DE IMPLEMENTACION DE LA NORMA ISO 27001 EN UNA EMPRESA TECNOLOGICA, EN LA CIUDAD DE SANTO DOMINGO. CASO GRUPO PCDATA TECHNOLOGIES, AÑO 2013

II. PROBLEMA DE LA INVESTIGACION

2.1 Planteamiento del problema

La empresa PCDATA TECHNOLOGIES, debido a su naturaleza contiene informaciones confidenciales de sus clientes, que la divulgación de la misma podría ocasionar una demanda por el uso no apropiado de esta información, por tal motivo esta compañía se ve en la necesidad de implementar un sistemas de seguridad de la información, al fin de establecer las normativas y regulaciones acerca del uso de la información.

2.2 Formulación del problema

¿Cuál sería el resultado de implementar la norma ISO 27001 en una empresa tecnológica?

2.3 Sistematización del problema

1. ¿Cuáles son las ventajas de implementar la norma ISO 27001?
2. ¿Cuáles son las desventajas de implementar la norma ISO 27001?
3. ¿Cuáles son los riesgos que incurre la empresa por no implementar la norma ISO 27001?
4. ¿Cuáles son los pasos requeridos para implementar la ISO 27001 en una empresa?

5. OBJETIVOS DE LA INVESTIGACION

3.1 Objetivo general

Elaborar una propuesta para implementar la norma ISO 27001 en una empresa tecnológica. Caso: GRUPO PCDATA TECHNOLOGIES.

3.2 Objetivos específicos

- Examinar las ventajas de implementar la norma ISO 27001 en una empresa.
- Investigar cuales son las formas más efectivas para la implementación de la norma ISO 27001.
- Investigar acerca de las consecuencias de no implementar la norma ISO 27001 en una empresa que posee información confidencial.
- Indagar acerca de los requerimientos para poder mantener la certificación de la norma ISO 27001.
- Examinar las diferentes regulaciones exigida para poder obtener la certificación de la norma ISO 27001.

IV JUSTIFICACIÓN DE LA INVESTIGACION

La justificación será:

- **Teórica**

Existe documentación suficiente sobre la norma ISO 27001:2005 de documentación que se pueden encontrar en: libros, Revistas, manuales de procedimientos, Internet, seminarios y talleres.

- **Metodológica**

Para la realización de esta investigación serán utilizadas las siguientes metodologías y técnicas: entrevistas a los Gerentes, así como también la técnica de la observación.

- **Práctica**

Proveer a la alta Dirección de la empresa PCDATA TECHNOLOGIES una propuesta para la implementación de la norma ISO 27001:2005.

El presente trabajo ofrecerá información a las empresas que quieran incursionar en mejorar sus sistemas de gestión de la información basándose en la norma ISO: 27001: 2005.

V MARCO TEÓRICO O DE REFERENCIA

5.1 Marco Teórico

Según el British Standard Institute es una estructura probada para la gestión y mejora continua de las políticas, los procedimientos y procesos de la organización. Las empresas que operan en el siglo XXI se enfrentan a muchos retos, significativos, entre ellos: Rentabilidad, competitividad, globalización, velocidad de los cambios, capacidad de adaptación, crecimiento y tecnología.

Equilibrar estos y otros requisitos empresariales puede constituir un proceso difícil y desalentador. Es aquí donde entran en juego los sistemas de gestión, al permitir aprovechar y desarrollar el potencial existente en la organización.

La implementación de un sistema de gestión eficaz puede ayudar a:

- Gestionar los riesgos sociales, medioambientales y financieros.
- Mejorar la efectividad operativa.
- Reducir costos.
- Aumentar la satisfacción de clientes y partes interesadas.
- Proteger la marca y la reputación.
- Lograr mejoras continuas.
- Potenciar la innovación.
- Eliminar las barreras al comercio.
- Aportar claridad al mercado.

Revisado archivos investigativos desde de las fuentes bibliográficas de Internet se ha encontrado los siguientes trabajos.

"Implementación de un Sistema de Gestión de Seguridad de la Información basado en la norma ISO 27001, para la Intranet de la Corporación Metropolitana de Salud" elaborado por: Flor María Álvarez Zurita y Pamela Anabel García Guzmán Segovia. Trabajo realizado en Quito –Ecuador en el año 2007 en cuyas conclusiones dice lo siguiente:

El Sistema de Gestión de Seguridad de la Información se define para cada organización en base a los riesgos que esté expuesta y los aspectos intrínsecos de su funcionamiento, y debe alinearse con la actividad de la organización; para realizar de forma estructurada, sistemática y metódica la gestión de la seguridad de Tecnologías de Información; una adecuada monitorización de los recursos de la red permite determinar posibles cuellos de botella que derivarían en fallos del sistema y de seguridad, dando tiempo a planificar las ampliaciones o actualizaciones del sistema con la suficiente antelación.

No se considera necesario extender el SGSI a toda la organización, lo primordial es centrarse en los procesos principales de la organización donde la parte de las actividades relacionadas con la gestión de la información, que suele coincidir con las áreas de sistemas de la información donde la seguridad de la información que se gestiona es crítico para las actividades del desarrollo del negocio.

Mediante la planificación se logra una adecuada implementación del SGSI, en donde se analiza el negocio para determinar los activos más importantes, posteriormente se realiza un análisis de los riesgos que las amenazas y vulnerabilidades pueden generar, los cuales serán gestionados con controles apropiadamente implementados y criterios establecidos.

Asimismo para el establecimiento de seguridad de la información se considera tres pilares fundamenta les: tecnología, procesos y las personas: Las empresas comúnmente invierten grandes sumas de dinero en tecnología y definición de procesos, y se han descuidado del personal de la empresa convirtiéndose así en el eslabón más débil de la cadena de seguridad, por esta razón es fundamental concienciar y fomentar la cultura de la seguridad de la información.

5.2 Marco Conceptual

Documentación: Sirve para documentar la información necesaria para los usuarios del software y para desarrollos futuros. (Diccionario de la Lengua Española (1992), Vigésima primera edición, Madrid.)

Gestión Documental: Conjunto de actividades que permiten coordinar y controlar los aspectos relacionados con creación, recepción, organización, almacenamiento, preservación, acceso y difusión de documentos. (Patricia Russso Gallo, Gestión documental en las organizaciones, 2009)

Instrucciones de trabajo: Describen las operaciones que hay que realizar en cada proceso o en cada puesto de trabajo. Es un conjunto muy amplio de documentos que debe ser revisado cada vez que se modifica un proceso o un método de trabajo.
(http://www.zeusconsult.com.mx/pwmc/00000015.htm, consultado el 21 de mayo del 2013)

Procedimiento: Forma específica de llevar a cabo una actividad. (http://www.zeusconsult.com.mx/pwmc/00000015.htm, consultado el 21 de mayo del 2013)

Registros: Documento que proporciona evidencia objetiva de actividades realizadas o de resultados obtenidos.
(http://www.zeusconsult.com.mx/pwmc/00000015.htm, consultado el 21 de mayo del 2013).

Mapa de documentos: Es el inventario de los documentos que se mueven por la organización, su valor y sus características. (Patricia Russso Gallo, Gestión documental en las organizaciones, 2009).

Cuadro de clasificación: Es la clasificación de la documentación de la organización, no en función del tipo de documentación o temática. (Patricia Russso Gallo, Gestión documental en las organizaciones, 2009).

Manuales de política y procedimiento: Establecen un marco sistemático y pautas firmes para las actividades y los procesos específicos de una organización a fin de facilitar la implementación eficaz de la estrategia del negocio a nivel estratégico y operativo. (Andreas G. Koutoupis, documentación de controles internos, Internal Auditor, edición de octubre de 2007, Disponible en http://www.zeusconsult.com.mx/pwmc/00000015.htm, consultado el 21 mayo del 2013).

VI METODOLOGÍA DE LA INVESTIGACIÓN

a. Tipo de Estudio

Se realizara una investigación de nivel exploratorio, para determinar las condiciones actuales de la seguridad de los sistemas de información y de comunicación.

b. Método

El proceso investigativo será descriptivo para conocer con profundidad el problema, estableciendo sus causas y consecuencias así como las dificultades por lo que está atravesando.

c. Técnicas

Para recabar la información se utilizará técnicas como la observación y la entrevista con sus respectivos instrumentos que son el registro de datos y un cuestionario de entrevistas

c) Fuentes

Serán utilizadas **fuentes primarias,** tales como la realización de entrevistas, y consultas de libros y revistas.

Fuentes Secundarias: libros de texto e investigaciones disponibles en internet.

VII ÍNDICE TENTATIVO

VIII BIBLIOGRAFÍA

1. Diccionario de la Lengua Española (1992), Vigésima primera edición, Madrid.

2. Hiles, A. (2005) Business Continuity Best Practices. Rothsein Associates.Inc.

3. King, A.A., Lenox, M.J. y Terlaak, A.K. (2005). "The strategic use of decentralized institutions: Exploring certification with the ISO 27001 management standard", Academy of Management Journal, Vol. 48, núm. 6.

Referencias de Internet:

1. ISO/IEC ISO 27001:2005 (2007). Information technology –security techniques – Information security Management Systems Requirements Specification. Recuperado el 9 de Marzo del 2008 en http://ISO27000.es