FUNDAMENTOS DE ISO 27001 Y SU APLICACIÓN EN LAS EMPRESAS

Fundamentals of ISO 27001 and its application in enterprises

RESUMEN
En este artículo se 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 como implementar estas buenas prácticas en empresas pequeñas que no pueden realizar la certificación.
.

PALABRAS CLAVES: ISO (International Organization for Standardization), Planear – Hacer – Verificar – Actuar (PHVA), Sistema de Gestión de Seguridad de la Información SGSI, procesos, ISO 27000, ISO 2700.1

MARTHA ISABEL LADINO A.
Ingeniera de Sistemas y Computación
Estudiante Especialización en Redes de Datos
Universidad Tecnológica de Pereira
ladinoar@utp.edu.co

PAULA ANDREA VILLA S.
Ingeniera de Sistemas y Computación
Profesor Auxiliar
Universidad Tecnológica de Pereira
pavaji@utp.edu.co

ANA MARÍA LÓPEZ E.
Ingeniera Electricista.
Coordinadora Programa Ing. Sistemas y Computación.
Universidad Tecnológica de Pereira
anamayi@utp.edu.co

ABSTRACT
This article presents an overview of the fundamentals of the ISO 27001 standard and its application in organizations. As a case study presents an experimental implementation of the standard in an organization, this rule can be implemented in a company with the goal of obtaining certification or simply as best practice to improve some aspects of enterprise security. Additionally shown how to implement these best practices in small businesses that can not perform the certification.

KEYWORDS: *ISO (International Organization for Standardization), Plan - Do - Check - Act (PDCA), Security Management System ISMS Information, processes, ISO 27000, ISO 2700.1*

1. INTRODUCCIÓN

El amplio uso de las tecnologías de información en los negocios hace que cada vez sea más fácil la expansión de éstos. La comunicación con clientes que se encuentran en una ciudad o país diferente al de ubicación de la empresa, la posibilidad de realizar transacciones comerciales vía web y en general, la facilidad del uso de la tecnología y la globalización de la información para todas las personas ha contribuido a que las organizaciones crezcan cada vez más rápido. Sin embargo, toda esta cercanía y facilidad de uso de la tecnología ha generado ciertos problemas a las organizaciones, que día tras día son más vulnerables a las amenazas que se presentan en el medio, las cuales pueden llegar a convertirse en un verdadero riesgo para la organización afectando el correcto funcionamiento de las actividades del negocio.

Para contrarrestar dichas amenazas, las organizaciones deben generar un plan de acción frente a éstas. Este plan de acción es conocido como Sistema de Gestión de Seguridad de la Información (SGSI) y contiene los lineamientos que deben seguirse en la organización, los responsables y la documentación necesaria para garantizar que el SGSI sea aplicado y genere una retroalimentación.

La definición de SGSI se hace de manera formal en la norma ISO 27001, donde están los estándares y mejores prácticas de seguridad de la información.

2. IMPORTANCIA DE LA SEGURIDAD DE LA INFORMACIÓN

La información es el instrumento fundamental para el funcionamiento de las empresas y la operación de los negocios, esto hace que la información deba protegerse como el activo más importante de la organización. En la actualidad dado el incremento de la utilización del internet, la evolución de la tecnología y la falta de conocimiento para mitigar riesgos de ataques, ha generado innumerables amenazas que aprovechan vulnerabilidades de las empresas para materializar riesgos y generar un impacto negativo en las organizaciones, ocasionando que se pierdan alguna o todas las características que debe preservar la información: disponibilidad, integridad, confidencialidad. “La organización Anti-Virus Test, que presta servicios de

Fecha de Recepción: 25 de Enero de 2010
Fecha de Aceptación: 28 de Abril de 2010

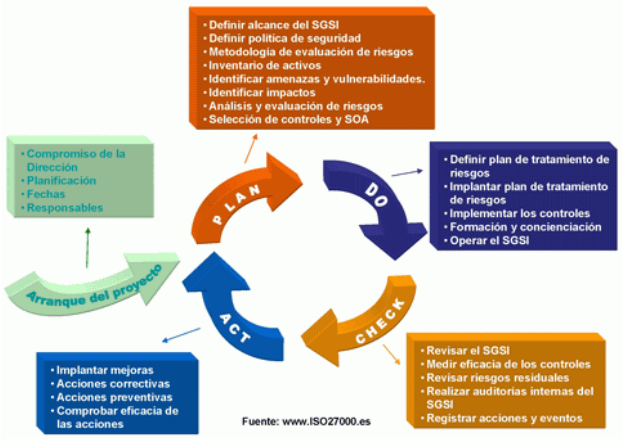
consultoría a empresas de seguridad informática, dice que en el 2008 habían 9 millones de Software malicioso en el mundo. En el 2009 la empresa registraba 22 millones, sólo de esta amenaza" [1].Con este panorama las empresas deben diseñar e implantar estrategias que les permita mejorar la seguridad de la información en su organización.

En Colombia ACIS (Asociación Colombiana de Ingeniería de Sistemas) realiza una encuesta nacional anualmente para conocer las tendencias en el tema de seguridad Algunas de las conclusiones de este estudio son: "La falta de apoyo directivo y la falta de tiempo, no pueden ser excusas para no avanzar en el desarrollo de un sistema de gestión de seguridad, la inversión en seguridad es costosa, pero la materialización de inseguridad puede serlo mucho más". "En Colombia el ISO 27000, ITIL y el Cobit 4.1 son el estándar y las buenas prácticas que están en las áreas de seguridad de la información o en los departamentos de tecnologías de información"[2], "se nota que poco a poco el mercado de especialistas en seguridad de la información toma fuerza, pero aún la oferta de programas académicos formales se encuentra limitada, lo que hace que las organizaciones opten por contratar a profesionales con poca experiencia en seguridad y formarlos localmente". Identificada la problemática anterior y según los resultados de estudios de mencionados es necesario diseñar estrategias que permitan a las empresas mejorar los mecanismos que poseen para preservar su activo más importante, la información. Como se mencionó anteriormente en Colombia el ISO 27000 es uno de los estándares más utilizados [3] y las regulaciones nacionales e internacionales llevarán a las organizaciones en Colombia a fortalecer los sistemas de gestión de la seguridad de la información, no solo para cumplir con lo establecido en la norma ISO 27001, sino en el diseño de sistemas más resistentes y confiables para los usuarios [4].

3. FUNDAMENTOS DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD 27001

La norma ISO 27000 es certificable. Esto significa que una empresa puede solicitar una auditoría a una entidad certificadora acreditada y si la supera, obtener la certificación. Antes de solicitar la auditoría las empresas necesitan contar con un Sistema de Gestión de Seguridad de la Información (SGSI). El SGSI debe estar implementado en la empresa como mínimo con tres meses de antelación.

Cada uno de los puntos exigidos en la norma pertenece a una etapa de un proceso: Plan – Do – Check – Act (Planificar-Hacer-Verificar-Actuar), que se aplica para estructurar todos los procesos del SGSI. El SGSI toma como elementos de entrada los requisitos de seguridad de la información y las expectativas de las partes interesadas, y a través de las acciones y procesos necesarios produce resultados de seguridad de la información que cumplen estas expectativas.
La siguiente figura muestra los puntos y a qué etapa del proceso pertenece cada uno:



Tomado de www.iso27000.es [5]

Sin embargo, al momento de realizar la auditoría, a algunos puntos se les da más relevancia que a otros:

- ✓ *Política de seguridad:* debe incluir los objetivos de seguridad de la información de la organización, tener en cuenta los requisitos de negocio, legales y contractuales en cuanto a seguridad, estar alineada con la gestión de riesgo general, establecer criterios de evaluación de riesgo y ser aprobada por la Dirección.

- ✓ *Asignación de responsabilidades de seguridad:* En toda actividad debe existir un responsable. Durante el proceso de certificación cada tarea debe estar definida para que una o unas personas de la organización la realicen.

- ✓ *Formación y capacitación para la seguridad:* debe realizarse una concienciación de todo el personal en lo relativo a la seguridad de la información.

- ✓ *Registro de incidencias de seguridad:* durante el proceso, debe realizarse un registro de los eventos casuales (incidencias), y determinar su impacto y frecuencia. Determinar controles de detección y respuesta a dichos incidentes.

- ✓ *Gestión de continuidad del negocio:* el SGSI definido, debe estar enfocado en mantener la continuidad del negocio, por lo tanto este objetivo no puede perderse en el camino de implementación del sistema de seguridad.

- ✓ *Salvaguarda de registros de la organización:* la información hace parte de los activos de la organización, por lo tanto ésta debe preservarse y

cuidarse como tal. Los registros de la organización ya sea del negocio o relacionados con el sistema de seguridad deben cumplir con las propiedades fundamentales: confidencialidad, integridad y disponibilidad.

- ✓ *Protección de datos personales:* hacen parte de la información de la organización y por ello deben ser protegidos.

- ✓ *Derechos de propiedad intelectual:* contar con las licencias y/o permisos para el uso de software en la organización.

Después que se ha implantado el SGSI en la organización, ésta solicita la auditoría a la empresa certificadora, la cual se realiza en varias fases:

- ✓ Pre-*auditoría:* es opcional, ayuda a recoger información sobre el estado de la organización antes de la auditoría real.
- ✓ *Fase 1 de la auditoría:* análisis de la documentación por parte del Auditor Jefe y la preparación del informe de la documentación básica del SGSI del cliente, destacando los posibles incumplimientos de la norma que se verificarán en la Fase 2. Este informe se envía junto al plan de auditoría al cliente. El periodo máximo entre la Fase 1 y Fase 2 es de 6 meses.
- ✓ *Fase 2 de la auditoría:* es la fase de detalle de la auditoría, en la que se revisan las políticas, la implantación de los controles de seguridad y la eficacia del sistema en su conjunto. Se realiza una revisión de las exclusiones según la Declaración de Aplicabilidad (documento SOA), de los hallazgos de la Fase 1, de la implantación de políticas, procedimientos y controles y de todos aquellos puntos que el auditor considere de interés. El resultado es el informe de auditoría.
- ✓ *Certificación:* en el caso de que se descubran durante la auditoría no conformidades graves, la organización deberá implantar acciones correctivas; una vez verificada dicha implantación o en el caso de no haberse presentado inconformidades, el auditor podrá emitir un informe favorable y el SGSI de organización será certificado según ISO 27001. [6]

Después de obtener la certificación debe hacerse un seguimiento, y realizar auditorías semestrales o anuales para verificar que el SGSI si se usa en la organización. La certificación debe renovarse cada tres años realizando nuevamente todo el proceso de auditoría.

El auditor es la persona que comprueba que el SGSI de una organización se ha diseñado, implementado, verificado y mejorado conforme a lo detallado en la norma. En general, hay tres clases de auditores: auditor interno (de primera parte), pertenece a la organización, realiza auditorías como mantenimiento del sistema de gestión y como preparación a la auditoría de certificación. Auditor de cliente (de segunda parte), audita una organización en nombre de un cliente de ésta. Finalmente está el auditor independiente (de tercera parte), que audita una organización como tercera parte imparcial; normalmente, porque la organización tiene la intención de lograr la certificación.

El auditor, sobre todo si actúa como de tercera parte, ha de disponer también de una certificación personal. Esto quiere decir que, nuevamente un tercero, certifica que posee las competencias profesionales y personales necesarias para desempeñar la labor de auditoría de la materia para la que está certificado.

El proceso de certificación es largo, complejo y costoso, por lo que algunas empresas no pueden realizarlo. Sin embargo pueden aplicar algunos puntos claves para lograr un buen nivel de seguridad. Aunque el término *buen nivel* es subjetivo, sobre todo por el desconocimiento del impacto negativo que pueda traer un riesgo que se materializa.

Algunas recomendaciones que deben tenerse en cuenta al momento de implementar un sistema de seguridad en la organización son las siguientes:

- ✓ La primera de ellas y tal vez la más importante, es el conocimiento de los altos directivos de lo que puede suceder si no se implementa el sistema de gestión de seguridad de la información. A la alta dirección debe hablársele en términos del negocio, es decir, demostrar las pérdidas económicas, que pueden tenerse en caso de no contar con un SGSI. De esta tarea puede encargarse el jefe del área de sistemas de la organización.

- ✓ Se debe realizar una identificación de los activos relacionados con la información, desde los equipos que la soportan hasta las aplicaciones para su uso y la información misma. Después identificar los más críticos para la compañía y con base en estos empezar la tarea de diseño e implementación del SGSI.

- ✓ Cuando las directivas de la organización tiene claro la necesidad de implantar un SGSI y han identificado los componentes críticos entre los activos, debe fomentarse una *cultura de seguridad* con todos los miembros de la organización para minimizar los riesgos por desconocimiento. Se debe tener en cuenta que plasmar en un papel algunas normas de seguridad no crean una cultura, es un proceso que debe realizarse de manera constante, ya que para generar cultura es necesario crear conciencia del cambio.

- ✓ Los expertos en el área de seguridad (jefe de área y otros trabajadores) deben ser los encargados de identificar las amenazas y debilidades que afectan a cada uno de los activos críticos. De esta forma se pueden definir los riesgos que afectan el proceso normal de la organización, incluyendo el impacto y la frecuencia con la que puedan ocurrir.

- ✓ Cuando se definen los riesgos, debe tenerse en cuenta que es imposible evitar o controlarlos todos, por eso en la organización debe definirse un *nivel aceptable de riesgo*, es decir, definir cuáles son los riesgos que se pueden asumir ya que no generarán un impacto muy negativo para el funcionamiento correcto de las actividades de la organización. La definición del nivel aceptable de riesgo debe estar bajo la responsabilidad directa de la alta gerencia de la organización y estar enfocado en el negocio y el cliente.

- ✓ Con los riesgos, el impacto, la frecuencia y el nivel aceptable se definen entonces, los controles que deben seguirse para evitar o minimizar los riesgos. Estos controles se enfocan en reducir el impacto, la frecuencia o evitar que el riesgo se materialice y cause un daño al correcto funcionamiento del negocio, que finalmente se verá reflejado en una pérdida o gasto económico.

Todo esto hace parte del Sistema de Gestión de Seguridad de la Información (SGSI), pero como ya se indicó anteriormente, es algo que no debe quedar sólo escrito. Hasta ahora se tiene únicamente el diseño.

- ✓ Después de tener el diseño del sistema de seguridad, debe empezar a aplicarse en la organización, Para esto es necesario promover la capacitación de las personas que laboran en la organización, comprar e implantar los equipos y aplicaciones necesarios.

- ✓ Para que la implementación sea efectiva, debe hacerse un seguimiento a los controles y, para lograr este seguimiento es necesario la *documentación* de los procesos y de los hallazgos. Con esta información se realiza una retroalimentación para corregir errores que aún se mantienen y mejorar el SGSI incluyendo nuevos riesgos posibles o restándole importancia a aquellos que se han logrado minimizar.

Aunque estas recomendaciones parezcan demasiado complicadas, son más fáciles, y económicas, de implementar que la norma completa para lograr la certificación (especialmente si se trata de empresas pequeñas y medianas) ya que, para esta segunda es necesario, generalmente, la intervención de un tercero que ayude en el proceso como asesor.

4. HERRAMIENTAS PARA MODELAR PROCESOS DE LA NORMA ISO 27001

A continuación se presenta un resumen de algunas herramientas que soportan la implantación de la norma ISO 27001 en las empresas, estas herramientas funcionan basadas en procesos.

NOMBRE: Gesttic
VERSIÓN: Gesttic Oro
CIUDAD: Vilassar de Mar (Barcelona)
FUNCIONALIDADES: Gestor de documentación
Cuadro de Mando Integral
Intranet corporativo
Gestor de Work flows
Extranet
Gestor de Proyectos

VENTAJAS:
1. Es un Gestor Documental multilingüe
2. Es adaptado a la Gestión de Sistemas de Calidad y Medio Ambiente "Sin Papeles"

CARACTERÍSTICAS TÉCNICAS:

Viene con 20h de formación. Incluye 5 usuarios, 100 MB de disco duro y 300 MB de tráfico mensual. Puede adquirir ampliaciones de usuarios.

TIPO DE CERTIFICACIONES:

1. OEA
2. ISO 9004
3. SICTED
4. ISO 9001
5. UNE EN 13816
6. UNE 187001
7. ISO 14001
8. EMAS: Eco Management and Audit Scheme
9. ISO 27001

SECTOR: Servicios, Público, Productivo
SOPORTE: 60 EUROS MES
PRECIO: 150 EUROS

NOMBRE: ISOTools
VERSIÓN: ISOTools Project Manager
CIUDAD: Madrid, Sevilla, Córdoba
FUNCIONALIDADES:

1. Gestión de proyectos
2. Gestión de tiempos
3. Gestor de tareas
4. Gestor de costes
5. Gestor del riesgo
6. Gestor de la calidad
7. Gestión de Recursos
8. Gestor de adquisiciones

VENTAJAS:

Eficacia: Mejora de la eficacia, permitiendo una perfecta gestión del conocimiento a nivel organizativo y documental.
Dinamismo: Sistemas de gestión dinámicos enfocados hacia la mejora continua y a la obtención de resultados.
Organización: Una agenda le permite planificar y avisar de todo lo que tiene que hacer.
Ahorro: Reduce los tiempos y costos de implantación y mantenimiento, optimizando la eficiencia de la mejora continua.
Accesibilidad: Disponibilidad de la información en cualquier momento y desde varios dispositivos.
Agilidad: Consultas rápidas de toda la información y tareas del sistema.
Centralización de la información: un dato único. Facilita la gestión del conocimiento de la organización Funcionalidad para la ISO 27001 Evaluación de Seguridad de la Información, Controles 27002, Salvaguardas, Métricas e Indicadores, Cuadro de Mando Colaboración: Potencia el flujo interno de comunicación y la involucración de todo el personal.

TIPO DE CERTIFICACIONES:

1. ISO 9001
2. ISO 14001
3. OHSAS 18001
4. ISO 27001
5. ISO 9004

SECTOR:

ISOTools es una herramienta estándar y personalizable por lo que es válida para la gestión de cualquier tipo de organización:
Empresas
Organismos Públicos
Asociaciones

SOPORTE: 28 EUROS MES
PRECIO: 15.330 Euros

NOMBRE: Process Maker

FUNCIONALIDADES:
Software para definición, gestión de procesos y flujos de trabajo.

- ✓ Diseño de Flujos de trabajo
- ✓ Creación Dinámica de formularios (Dynaform)
- ✓ Gestión de Casos y reportes
- ✓ Código fuente abierto
- ✓ Integración a otros sistemas.
- ✓ Basado en web, por lo que no requiere instalación, por lo tanto se debe contar con un servidor donde pueda operar el software.
- ✓ Interface AJAX de fácil uso para la creación simple de procesos y tener una vista previa instantánea.
- ✓ Integración con bases de datos como MySql, Oracle, MSSQL.
- ✓ Fácilmente adaptable a cambios

5. CASO PRÁCTICO DE LA IMPLEMENTACIÓN DE LA NORMA ISO 27000 EN UNA ORGANIZACIÓN

A continuación se presenta una experiencia general compartida por un asesor que ha participado del proceso de certificación de la norma ISO 27001 en una entidad pública.

"En la organización empezamos a verificar que los controles de la norma se estuvieran efectuando, pero después de varias evaluaciones notamos que las personas involucradas no estaban cumpliendo muchos procesos que estaban ya definidos con anticipación, entonces el comité decidió para la implantación de la norma dirigirse al departamento de sistemas y se definió que era necesario implementar algunos controles desde el software que estaban utilizando, para obligar a los usuarios a cumplir con los mencionados procesos. En la entidad ya estaba establecido el sistema de gestión de calidad (ISO 9001) y lo que hicimos fue adherir los procesos de seguridad a este sistema, dado que es lo que comúnmente realizan las empresas, además la tendencia es tener un sistema integral de gestión llamado Human Security Enviroment Quality (HSEQ) el cual está compuesto por un conjunto de normas ISO que se refieren a recursos humanos, seguridad, medio ambiente y calidad, no es necesario tenerlas todas implementadas, eso va a depender del tipo de organización "

Con la información de la experiencia anterior se evidencia que es complicado cambiar la forma de trabajo de las personas de la organización y esto complica la implantación del sistema sino se realiza la gestión del cambio de forma adecuada.

6. CONCLUSIONES

Dado que ahora la información es considerada como el activo más importante de la organización es imprescindible protegerlo contra las amenazas que se encuentran en el medio.

No es obligatorio en Colombia aún que una organización obtenga certificación en la norma ISO 27001 a diferencia de otros países latinoamericanos, pero es necesario implementar buenas prácticas que permitan establecer controles para proteger las características de la seguridad de la información.

Existen diversas herramientas tanto libres como privativas que apoyan el sistema de gestión de seguridad de la información, optimizando procesos o actividades.

La experiencia demuestra que se puede llevar a cabo la implementación e implantación del sistema de gestión de seguridad de la información en una organización si se realiza teniendo en cuenta la gestión del recurso humano.

7. BIBLIOGRAFÍA

[1]http://www.vanguardia.com/archivo/48183-seguridad-informatica-en-2010

[2]http://www.acis.org.co/fileadmin/Revista_110/05investigacion1.pdf
http://www.acis.org.co/fileadmin/Revista_101/investigacion.pdf

[3] Seguridad de la Información en Latinoamérica Tendencias 2009.http://www.acis.org.co/fileadmin/Revista_110/05investigacion1.pdf

[4] VII Encuesta Nacional de Seguridad Informática.http://www.acis.org.co/fileadmin/Revista_101/investigacion.pdf

[5]http://www.iso27000.es/certificacion.html#section5b

[6]http://www.business-intelligent.com/iso27000.pdf

[7] Norma ISO 27000. Traducida al español en 2006

[8] Chi-Hsiang Wang. Integrated Installing ISO 9000 and ISO 27000 Management Systems on an Organization. IEEE

[9] Manik Dey. Information Security Management - A Practical Approach. IEEE.

[10] Wolfgang BOEHMER. Cost-benefit trade-off analysis of an ISMS based on ISO 27001.IEEE

[11] Carlos S. Álvarez C. La ley y la seguridad de la información: una perspectiva regional. ACIS

[12] Sara Gallardo M. Monitoreo y cumplimiento en la Seguridad de la información. ACIS

[13] Andrés Ricardo Almanza Junco Ms(c).Convergencia de la seguridad