Universidad Nacional Experimental del Táchira

Vicerrectorado Académico

Decanato de Docencia

Departamento de Ingeniería en Informática

Seminario

Implantación y Certificación de un SGSI

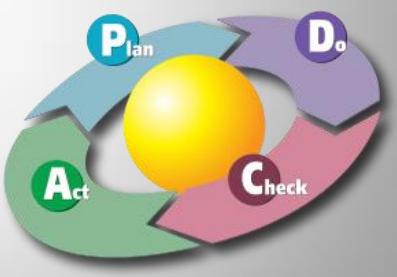
Cardelli M. Tyson J. CI: 23.542.402

Heredia C. Joel X. CI: 20.123.873

Rangel C. Carlos A. CI: 21.003.721

24/07/2016

"Un sistema de gestión de seguridad de la información consiste en las políticas, procedimientos, directrices, recursos y actividades gestionados colectivamente por una organización en la búsqueda de proteger sus activos de información " ISO/IEC 27000:2014(E)



Implantación y Certificación de un SGSI

Como parte de una organización es de vital importancia preguntarse ¿Está mi información segura? ¿Qué puede ocurrir si se pierde o se roban mi información? ¿Cuánto dinero se ve comprometido? Si acabas de hacerte estas preguntas y tu respuesta fue alarmante, entonces debes empezar a considerar la implantación de un SGSI (Sistema de gestión de seguridad de información).

La mayoría de las empresas le dan gran importancia a sus bienes materiales físicos, sin darse cuenta que en lo intangible esta lo más valioso de la organización. Según **"ISO/IEC 27000, Information security management systems — Overview and vocabulary**" La información es un activo que como otros activos de la de una organización es esencial y la cual puede ser almacenada en diferentes formas tanto digital como material y son numerosos los medios por los cuales puede ser transmitida.

La seguridad de la información incluye tres pilares fundamentales los cuales son integridad, confidencialidad y disponibilidad, los cuales se deben garantizar a través de sistemas de control. El ciclo de Deming PDCA (Plan, do, check, act) es un círculo de mejora continua basado en un concepto ideado por Walter A Shewhart y permite mejorar la calidad, reducir costos, optimizar la productividad y garantizar la seguridad de la información aumentando la rentabilidad de la empresa

PLAN (Planificar)

- ✓ Inicialmente se debe obtener soporte de la alta gerencia, en él se aplica la norma **ISO/IEC 27001:2013** en su apartado 5.1, en esta etapa se debe mantener el registro de las decisiones de la dirección. Como también establecer un procedimiento de gestión documental. El soporte de la alta gerencia es de vital importancia, ya que va a monitorear el cumplimiento del proceso y velar por la mejora continua.

- ✓ Se debe definir el alcance el SGSI, igualmente según la norma **ISO/IEC 27001:2013** en su apartado 4.3 se puede ampliar la información, sin embargo su objetivo fundamental es comprender las expectativas de las partes interesadas, de esta forma se podrán identificar los problemas externos e internos de manera que satisfaga las actividades desempeñadas por la organización en cada una de sus dependencias.

- ✓ Definir el alcance conlleva realizar la política para el SGSI, el cual es una declaración de intenciones, que incluye objetivos, requisitos de negocio, contexto estratégico y la cual debe ser aprobada por la dirección.

- ✓ Se debe realizar un sistema de control de inventarios de la información (Conocer que información es valiosa para la organización), se puede ampliar información en **http://www.iso27000.es/sgsi_implantar.html#seccion1**

- ✓ Paso siguiente se debe identificar la metodología para identificar los riesgos de la organización. Según **ISO 27001:2005** no se impone ninguna para que cada organización tome la que considera más oportuna. Igualmente se recomienda profundizar sobre el tema con la norma **ISO 27005** ya que profundiza en cómo debe hacerse la valoración de riesgos en cuanto a probabilidad, ocurrencias, consecuencias y proximidad.

- ✓ Después de tener claro la metodología a utilizar se debe hacer el análisis de riesgos, es importante hacer énfasis en que el análisis de riesgos se **"hace"** durante esta etapa de planificación, esta fase generará reportes de riesgos que son de vital importancia para continuar el proceso de mejora continua

- ✓ Según **http://www.iso27000.es/sgsi_implantar.html#seccion1** analizar y evaluar los riesgos implica evaluar el impacto del negocio ante un fallo de seguridad, evaluar de forma realista la probabilidad de ocurrencia e identificar los criterios de aceptación del riesgo.

- ✓ Para finalizar esta etapa se debe definir los **controles** a utilizar teniendo en cuenta un plan para el tratamiento de riesgos anteriormente identificados, para ello se recomienda ampliar la información acerca de controles de seguridad en la **ISO27002:2005 segunda clausula** la cual proporciona una guía completa de 133 controles según 39 objetivos agrupados en 11 dominios. E incluso deja abierta la posibilidad de implementar otros controles en caso de que alguno no se ajuste a los requerimientos de la organización.

- ✓ Como paso paralelo se debe preparar la declaración de aplicabilidad SOA (Statement of Applicability) la cual va a contemplar los objetivos de los controles seleccionados, aquellos que ya están implantados y el porqué de aquellos que se descartaron

Es importante hacer énfasis en el proceso de documentación y su importancia pues muchas organizaciones carecen de controles adecuados, por ejemplo también se recomienda revisar **ISO27001:20013 ANEXO A** en su apartado de objetivos de control y controles, el cuadro comparativo que allí se referencia toca aspectos muy importantes sobre controles, por ejemplo para el caso de inventario de activos se hace referencia a controles como propiedad de los activos (todo activo debe tener un propietario) uso aceptable de activos y la manera adecuada en que se debe hacer el inventario y la devolución de los mismos. Enmarcar la organización en los estándares de la ISO27000 garantizara el éxito de la misma.

DO (Hacer) Implantar y utilizar el SGSI:

"Se realizan los cambios para implantar la mejora propuesta. Generalmente conviene hacer una prueba piloto para probar el funcionamiento antes de realizar los cambios a gran escala." – Tomado **de http://www.pdcahome.com/5202/ciclo-pdca/**

"Aquí se lleva a cabo lo planeado. Siguiendo lo estipulado en el punto anterior, se procede a seguir los pasos indicados en el mismo orden y proporción en el que se encuentran indicados en la fase de planificación." – Tomado de **http://www.sbqconsultores.es/el-ciclo-de-deming-o-circulo-pdca/**

La documentación establece que para ésta etapa se deben implementar los nuevos procesos, a una pequeña escala.

Según **http://www.iso27000.es/sgsi_implantar.html#seccion2**

- ✓ Se debe garantizar que en el plan de tratamiento de riesgos definido se identifique:
  - Acciones
  - Recursos
  - Responsabilidades
  - Prioridades

Para tener una correcta gestión de los riesgos de seguridad de la información. En esta etapa también se debe:

- ✓ Implantar el plan de tratamiento de riesgos para los objetivos de control identificados, contemplando de igual manera la asignación de los recursos, la designación responsabilidades y prioridades.
- ✓ Llevar a cabo la implementación de los controles anteriormente seleccionados que satisfagan los objetivos de control.
- ✓ Definir y diseñar un sistema de métricas que permita obtener y monitorear los resultados, y de esa manera medir la eficacia de los controles o grupos de controles.
- ✓ Para obtener una implementación exitosa de los controles y minimizar los riesgos es necesario que la empresa cree programas de formación y concienciación para todo el personal en relación a la seguridad de la información.
- ✓ Gestionar las operaciones del SGSI.
- ✓ Gestionar los recursos necesarios asignados al SGSI para el mantenimiento de la seguridad de la información (no debe escatimarse en gastos para el SGSI).
- ✓ Implantar procedimientos y controles que permitan una rápida detección y respuesta a los incidentes de seguridad.
- ✓ Desarrollo del marco normativo necesario: normas, manuales, procedimientos e instrucciones.

Cada uno de los ítems anteriormente listados son etapas recomendadas por **ISO27000**, es importante tomar en cuenta que además de llevar a cabo cada uno de ellos se necesita establecer una correcta documentación, a fin de tener claridad y confiabilidad de todo el proceso.

El plan de implementación y certificación de ISO27000 se recomienda tener la siguiente documentación:

- ✓ Procedimientos de auditoría interna del SGSI.
- ✓ Procedimientos de acciones preventivas.
- ✓ Documentación de los controles y procesos.
- ✓ Métricas del Sistema
- ✓ Procedimientos operativos del SGSI.
- ✓ Procedimientos de control de registros.
- ✓ Procedimientos de acciones correctivas.

CHECK (Revisar)

Es en esta fase es donde se lleva a cabo todo el proceso de verificación y revisión por parte de la dirección del cumplimiento de los objetivos propuestos, el alcance proyectado, las medidas de seguridad implementadas para mitigar los riesgos. El proceso de seguimiento y monitorización del SGSI se hace con base a los resultados que arroja los indicadores de la seguridad de la información propuestos para verificación de la eficacia y efectividad de los controles implementados.

La revisión del SGSI por la dirección debe realizarse en forma planificada por lo menos en forma anual. Así mismo los resultados de la revisión por la dirección debe incluir cualquier decisión y acción relacionada con la mejora de la eficacia del SGSI, la actualización de la evaluación de los riesgos y el plan de tratamiento de riesgos, con ello elaborar los registros de la revisión al SGSI.

En esta etapa se realizan auditorías internas para la revisión del SGSI implantado, de forma planificada con la finalidad de verificar que los objetivos de control, controles, procesos y procedimientos del SGSI cumplen con los requisitos de la norma y así se verifica la exactitud y corrección de los cambios introducidos en el sistema con el fin de mantener un registro de las acciones y eventos que conlleven a la obtención de un plan de mejoras.

En esta fase se deben ejecutar principalmente las siguientes acciones:

Revisión del Cumplimiento: Esta actividad se realiza periódicamente en la organización para determinar si se está cumpliendo con lo establecido en la planificación de esta manera poder realizar los ajustes si están presentando desviaciones en lo planeado, por otra parte también permite detectar posibles problemas dentro de la organización que necesitan corregirse.

Acciones correctivas: Se realizan una vez detectados desfases entre lo planeado y la realidad, pues tal vez se estimaron mal los riesgos o los controles aplicados no son suficientes. En este punto se debe hacer uso del procedimiento de acciones correctivas para la eficaz aplicación de las mismas.

Valoración de Pre-certificación: Es un punto opcional muy recomendable en el cual se revisa de cerca el sistema de seguridad de la información existente y lo compara con los requisitos del estándar ISO/IEC 2700, lo que ayuda a identificar el grado de implementación y las áreas que necesitan más trabajo antes de llevar a cabo la auditoría formal,

Auditoría de Certificación: La certificación ISO/IEC 27001 consiste en realizar una auditoría oficial al sistema de gestión. La cual se lleva a cabo a través de dos fases, una fase inicial en la que se den revisiones a la documentación que soporta al sistema para verificar si se han desarrollado los procedimientos y controles ISO/IEC 27001. Y una segunda fase en donde el auditor evaluará las políticas, la implantación de los controles de seguridad y la eficacia del sistema en su conjunto,, para asegurar que estén funcionando eficientemente como lo requiere la certificación. Durante estas auditorías pueden surgir inconformidades, errores del sistema, o no conformidades. Las cuales deben ser presentadas por la organización en un Plan de Acciones Correctivas por cada inconformidad detectada que incluya un análisis de las causas raíz que originaron la desviación.

ACT (Mantener y Mejorar)

El propósito principal de ésta fase es mantener el SGSI y establecer mejoras con el paso del tiempo, dado que ningún sistema va a estar 100% seguro, ya que con el paso del tiempo nuevas amenazas han de surgir, el principal beneficio de tener un SGSI óptimo es el de reducir los riesgos que esto conlleva y en caso de detectar amenazas poder tomar las acciones correctivas con facilidad.

Según **http://www.iso27000.es/sgsi_implantar.html#seccion4** en ésta fase se debe realizar lo siguiente:

- Implantar en el SGSI las mejoras identificadas.
- Realizar las acciones preventivas y correctivas adecuadas para prevenir potenciales no conformidades antes de que se produzcan y solucionar no conformidades detectadas y materializadas. en relación a la cláusula 8 de ISO 27001:2005 y a las lecciones aprendidas de las experiencias propias y de otras organizaciones.
- 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: la eficacia de cualquier acción, medida o cambio debe comprobarse siempre.

Se debe tomar en consideración que el ciclo presentado para la implantación de un SGSI es un proceso de continuas mejoras, que se traducen en la continuidad del negocio, su correcta implementación hará que la empresa tenga sus procesos ordenados y por tanto sus índices de eficiencia y eficacia superen las expectativas.