Universidad Nacional de la Amazonía Peruana

Facultad de Ingeniería de Sistemas e Informática

“Metodologías de Implementación de un SGSI”

INFORME PRÁCTICO DE SUFICIENCIA

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO DE SISTEMAS E INFORMÁTICA

PRESENTADO POR EL BACHILLER:

EMIR MANUEL FLORES NAVAS

IQUITOS – PERÚ

2016

Universidad Nacional de la Amazonía Peruana
Facultad de Ingeniería de Sistemas e Informática

MIEMBROS DEL JURADO EXAMINADOR:

ING. JOSÉ EDGAR GARCÍA DÍAZ
PRESIDENTE

ING. ALEJANDRO REÁTEGUI PEZO
PRIMER MIEMBRO

LIC. ADM. ÁNGEL ILDEFONSO CATASHUNGA TORRES
SEGUNDO MIEMBRO

Tema: Metodologías de Implementación de un SGSI 2
Autor: Emir Manuel Flores Navas

UNIVERSIDAD NACIONAL DE LA AMAZONIA PERUANA
FACULTAD DE INGENIERIA DE SISTEMAS E INFORMATICA

ACTA DE EXAMEN ORAL DE SUFICIENCIA PROFESIONAL

Siendo las 19:40 horas del día 03 de NOVIEMBRE del 2016, en las instalaciones del Auditorio de la Facultad de Enfermería de la Universidad Nacional de la Amazonia Peruana, el Jurado Examinador, compuesto por los siguientes miembros:

Presidente : Ing. José Edgar García Díaz
Primer Miembro : Ing. Alejandro Reátegui Pezo
Segundo Miembro : Lic. Adm. Ángel Ildefonso Catashunga Torres

SECRETARIA ACADEMICA FISI - UNAP

Posteriormente se procedió al acto académico del examen oral de suficiencia profesional del bachiller: **Emir Manuel Flores Navas**, quien sustento el tema; **"Metodología de un Sistema de Gestión de Sistema de Información"**.

EMIR MANUEL FLORES NAVAS

Se procedió al cálculo de la Calificación y Condición Final, obteniéndose el siguiente resultado:

	Calificaciones	
	En número	**En letras**
Promedio de la Calificación Final de las Asignaturas.	14.33	CATORCE Y 33/100
Calificación de la Sustentación del Informe Final.	17.33	DIECISIETE Y 33/100
Calificación Final	15.83	QUINCE Y 83/100

Se desprende que la Condición Final del Bachiller es (marcar el que corresponde):

( ) Aprobado con excelencia (18 a 20 puntos).
(X) Aprobado por unanimidad (15 a 17.9 puntos).
( ) Aprobado por mayoría (12 a 14.9 puntos).
( ) Desaprobado (Menos de 12 puntos).

Siendo las 20:15 horas del mismo día, se da por concluido el acto, firmando en conformidad los miembros del Jurado Examinador.

Presidente

Primer Miembro

Segundo Miembro

AGRADECIMIENTO

A Dios, primero por darme la vida, por haber inspirado mi espíritu para que pueda concluir este informe práctico y por guiarme en cada paso que doy en mi carrera profesional.

A mis Padres, Por haberme forjado como la persona que soy en la actualidad, por sus consejos, su apoyo incondicional y su paciencia, todos mis logros se los debo a ustedes incluyendo este.

A mis Hermanos, por el apoyo que siempre me brindaron día a día en el transcurso de cada año de mi carrera universitaria.

Y a mis amigos, por estar siempre conmigo.

RESUMEN

Los **Sistemas de Información** hoy en día están cada vez más expuestos a una serie de amenazas que constituyen un riesgo sobre uno de los activos más importantes de las organizaciones como es la información. Asegurar la disponibilidad, la confidencialidad y la conservación de los datos, es un servicio que debe brindar la organización por lo que la gestión de la seguridad de la Información debe realizarse mediante un proceso documentado.

Un **Sistema de Gestión de la Seguridad de la Información (SGSI)**, definido por la norma **ISO/IEC 27001**, no solo debe considerar el contexto de la industria y características culturales de la organización, sino también debe ser sostenible en el tiempo, con capacidad de incorporar mejoras de forma incremental y continua, con un beneficio comprobable para la Organización.

La **Seguridad de la Información** es la protección de la información contra una amplia gama de amenazas; para minimizar los daños, ampliar las oportunidades del negocio, maximizar el retorno de las inversiones y asegurar la continuidad del negocio; y esto se va logrando mediante la implementación de un conjunto adecuado de políticas, procesos, procedimientos, organización, controles, hardware y software y lo más importante mediante el comportamiento ético de las personas.

Esta metodología nos va permitir, en primer lugar, analizar y ordenar la estructura de los sistemas de información y nos ofrecerá la posibilidad de disponer controles que permitan medir la eficacia de las medidas tomadas. Estas acciones van a proteger a nuestra organización frente a amenazas y riesgos que puedan poner en peligro la continuidad de los niveles de competitividad, rentabilidad y conformidad legal para alcanzar los objetivos de negocio de la organización.

Palabras claves: Sistema de Gestión de la Seguridad de la Información, Seguridad de la Información, ISO/IEC 27001.

Índice

I. JUSTIFICACIÓN

Es de gran importancia la información que manejan las organizaciones para mantener su integridad, confidencialidad y disponibilidad para alcanzar los objetivos de negocio. Grandes corporaciones o grupos empresariales del sector financiero, salud o gubernamentales están sujetos a riesgos o amenazas que puedan vulnerar sus recursos informáticos, con un elevado riesgo de sufrir un incidente de alto impacto en su actividad. El imparable avance de las nuevas tecnologías en las organizaciones y en general, el desarrollo de la era de la información agrava constantemente esta situación.

Por lo tanto la seguridad de la información es responsabilidad de la organización al ser el apoyo principal a establecer políticas y procedimientos en relación a los objetivos de negocio de la organización, con el propósito de mantener un nivel de riesgo mínimo.

De acuerdo con lo anterior es necesario diseñar una metodología para la implementación de **un sistema de gestión de seguridad de la información – SGSI**, teniendo como referencia la familia de las normas **ISO 27000**, para garantizar su disponibilidad, integridad y confidencialidad,

Este sistema permite identificar, gestionar y minimizar los riesgos reales y potenciales de la seguridad de la información por la organización de una forma documentada, sistemática, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías.

II. OBJETIVOS

OBJETIVO GENERAL

Elaborar una base teórica sobre el diseño de una implementación de un Sistema de Gestión de Seguridad de la Información aclarando cada fase y los estándares a seguir.

OBJETIVO ESPECÍFICOS

- Definir los conceptos que engloban los Sistemas de Gestión de Seguridad de Información.

- Describir el proceso a seguir para la implementación de un SGSI en una organización.

III. DESARROLLO DEL TEMA

3.1. INTRODUCCIÓN:

Los sistemas de información de las organizaciones desarrollan su misión en un entorno hostil. Las organizaciones son responsables de la protección de la información que gestionan ante las amenazas de este entorno y deben, por todos los medios disponibles, garantizar su confidencialidad, integridad y disponibilidad.

Desde hace tiempo, se percibe una creciente preocupación por todos los aspectos relacionados con la seguridad. Todas las organizaciones, públicas o privadas, grandes o pequeñas, se enfrentan día a día a amenazas contra sus recursos informáticos, con elevado riesgo de sufrir incidentes de alto impacto en su actividad.

Los riesgos que surgen relacionados con tecnologías y procesos, requieren soluciones y servicios emergentes. Soluciones para garantizar, de forma continua en el tiempo, la actividad de las organizaciones, la seguridad de la información base del negocio y los derechos de los individuos, en una sociedad cada vez más informatizada.

La seguridad no es un producto: es un proceso continuo que debe ser controlado, gestionado y monitorizado. Con el objetivo de ilustrar el contenido de la metodología que se planteen abordar una estrategia de seguridad de la información para proteger sus datos e información tomando como base fundamental el modelo de mejora continua PHVA fundamentado en la norma ISO/IEC 27001. Primeramente, se realiza la descripción del SGSI con la definición del escenario y la planeación (PLANEAR), el desarrollo del modelo desde su implementación hasta la gestión de la ejecución donde se fijan los controles y su aplicabilidad (HACER), después de que el SGSI se encuentra en marcha, se inician las actividades de monitorización y revisión (VERIFICAR) y finalmente se identifican las mejoras que se van hacer en el sistema (ACTUAR).

3.2. CONCEPTOS:

3.2.1. METÓDOLOGÍAS:

Una Metodología es un conjunto de procedimientos racionales utilizados para alcanzar el objetivo o la gama de objetivos que rige una investigación científica, una exposición doctrinal o tareas que requieran habilidades, conocimientos o cuidados específicos; Es una de las etapas específicas de un trabajo o proyecto que parte de una posición teórica y conduce una selección de técnicas concretas (o métodos) acerca del procedimiento destinado a la realización de tareas vinculadas a la investigación, el trabajo o el proyecto.

No debe llamarse metodología a cualquier procedimiento, pues se trata de un concepto que en la gran mayoría de los casos resulta demasiado amplio, siendo preferible usar el vocablo método. También es de saber que existe una posición a metódica e incluso una tendencia de matizado anarquismo epistemológico.

3.2.2. IMPLEMENTACIÓN:

Una implementación es la instalación de una aplicación informática, realización o la ejecución de un plan, idea, modelo científico, diseño, especificación, estándar, algoritmo o política.

En ciencias de la computación, una implementación es la realización de una especificación técnica o algoritmos como un programa, componente software, u otro sistema de cómputo.

En la industria IT, la implementación se refiere al proceso post-venta de guía de un cliente sobre el uso del software o hardware que el cliente ha comprado. Incluyendo el análisis de requisitos, análisis del impacto, optimizaciones, sistema de integración, política de uso, aprendizaje del usuario y costes asociado.

3.2.3. SISTEMA DE GESTIÓN DE LA SEGURIDAD DE INFORMACIÓN:

La seguridad de la información es la protección de los activos de la información de un rango amplio de amenazas para poder asegurar la continuidad del negocio, minimizar el riesgo comercial y maximizar el retorno de las inversiones y las oportunidades comerciales. Estos activos se pueden detallar como: correos electrónicos, páginas web, imágenes, base de datos, telecomunicaciones, contratos, documentos, etc.

La seguridad de estos activos de la información se logra implementando un adecuado conjunto de controles; incluyendo políticas, procesos, procedimientos, estructuras organizacionales y funciones de software y hardware. Se necesitan establecer, implementar, monitorear, revisar y mejorar estos controles cuando sea necesario para asegurar que se cumplan los objetivos de seguridad y comerciales específicos.

La gestión de seguridad de la información apunta a mantener la estabilidad en los siguientes aspectos con respecto a estos activos:

Confiabilidad: Acceso solo de personal autorizados.
Integridad: Exactitud y completitud de la información y procesos.
Disponibilidad: Acceso a la información y procesos por parte del personal autorizado, cuando lo requieran.

3.2.4. ORGANIZACION INTERNACIONAL DE ESTANDARIZACION (ISO)

La ISO es una federación internacional con sede en Ginebra (Suiza) de los institutos de normalización de 157 países (uno por cada país). Es una organización no gubernamental (sus miembros no son delegados de gobiernos nacionales), puesto que el origen de los institutos de normalización nacionales es diferente en cada país (entidad pública, privada).

Las normas ISO surgen para armonizar la gran cantidad de normas sobre gestión de calidad y seguridad que estaban apareciendo en distintos países y organizaciones del mundo. Los organismos de normalización de cada país

producen normas que resultan del consenso entre representantes del estado y de la industria. De la misma manera las normas ISO surgen del consenso entre representantes de los distintos países integrados a la I.S.O.

3.2.5. ISO 27000, APLICADA A LA SEGURIDAD DE LA INFORMACIÓN:

Uno de los activos más valiosos que hoy en día posee las diferentes empresas, es la información y parece ser que cada vez más sufre grandes amenazas en cuanto a su confiabilidad y su resguardo, de igual forma la información es vital para el éxito y sobrevivencia de las empresas en cualquier mercado. Con todo esto todo parece indicar que uno de los principales objetivos de toda organización es el aseguramiento de dicha información, así como también de los sistemas que la procesan.

Para que exista una adecuada gestión de la seguridad de la información dentro de las organizaciones, es necesario implantar un sistema que aborde esta tarea de una forma metódica y lógica, documentada y basada en unos objetivos claros de seguridad y una evaluación de los riesgos a los que está sometida la información de la organización. Para lograr estos objetivos, existen organizaciones o entes especializados en redactar estándares necesarios y especiales para el resguardo y seguridad de la información, los estándares correspondientes se encuentran en la norma ISO 27000.

La ISO 27000 es una serie de estándares desarrollados, por ISO e IEC. Este estándar ha sido preparado para proporcionar y promover un modelo para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de Información. La adopción de este estándar diseño e implementación debe ser tomada en cuenta como una decisión estratégica para la organización; se pretende que el SGSI se extienda con el tiempo en relación a las necesidades de la organización. La aplicación de cualquier estándar ISO 27000 necesita de un vocabulario claramente definido, que evite distintas interpretaciones de conceptos técnicos y de gestión, que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña.

3.2.5.1 SERIE ISO 27000:

ISO ha reservado la serie de numeración 27000 para las normas relacionadas con sistemas de gestión de seguridad de la información. En el 2005 incluyó en ella la primera de la serie (ISO 27001), las demás son:

- ISO27000 (términos y definiciones),
- ISO27002 (objetivos de control y controles),
- ISO27003 (se centra en aspectos críticos en la Implementación SGSI),
- ISO27004 (desarrollo y utilización de métricas y técnicas de Medida de la efectividad de un SGSI),
- ISO27005 (directivas guía para la gestión del riesgo de Seguridad de la información)
- ISO27006 (proceso de acreditación de entidades de Auditorías, certificación y el registro de SGSI).
- ISO/IEC 27007 Guía de Auditoria de un SGSI

3.2.6. ISO 27001

Es un estándar ISO que proporciona un modelo para establecer, implementar, operar, supervisar, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI). Se basa en el ciclo de vida PDCA (Planear-Hacer-Verificar-Actuar) de mejora continua, al igual que otras normas de sistemas de gestión.

Este estándar es certificable, es decir, cualquier organización que tenga implantado un SGSI según este modelo, puede solicitar una auditoría externa por parte de una entidad acreditada y, tras superar con éxito la misma, recibir la certificación en ISO 27001.

El origen de la Norma ISO27001 está en el estándar británico BSI (British StandardsInstitution) BS7799- Parte 2, estándar que fue publicado en 1998 y era certificable desde entonces. Tras la adaptación pertinente, ISO 27001 fue publicada el 15 de octubre de 2005.

El enfoque del proceso para la gestión de la seguridad de la información presentado en este estándar internacional fomenta que sus usuarios enfaticen la importancia de:

- Entender los requerimientos de seguridad de la información de una organización y la necesidad de establecer una política y objetivos para la seguridad de la información.
- Implementar y operar controles para manejar los riesgos de la seguridad de la información.
- Monitorear y revisar el desempeño del SGSI
- Realizar mejoramiento continuo en base a la medición del objetivo

3.2.7. ISO 27002

ISO/IEC 27002 es un estándar para la seguridad de la información publicado por primera vez como ISO/IEC 17799:2000 por la ISO e IEC en el año 2000. Tras un periodo de revisión y actualización de los contenidos del estándar, se publicó en el año 2005 el documento actualizado denominado ISO/IEC 17799:2005.

ISO/IEC 27002 proporciona recomendaciones de las mejores prácticas en la gestión de la seguridad de la información a todos los interesados y responsables en iniciar, implantar o mantener sistemas de gestión de la seguridad de la información. La seguridad de la información se define en el estándar como "la preservación de la confidencialidad (asegurando que sólo quienes estén autorizados pueden acceder a la información), integridad (asegurando que la información y sus métodos de proceso son exactos y completos) y disponibilidad (asegurando que los usuarios autorizados tienen acceso a la información y a sus activos asociados cuando lo requieran)".

La versión de 2005 del estándar incluye las siguientes once secciones principales:

1. Política de Seguridad de la Información.
2. Organización de la Seguridad de la Información.
3. Gestión de Activos de Información.
4. Seguridad de los Recursos Humanos.
5. Seguridad Física y Ambiental.
6. Gestión de las Comunicaciones y Operaciones.
7. Control de Accesos.
8. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información.
9. Gestión de Incidentes en la Seguridad de la Información.
10. Gestión de Continuidad del Negocio.
11. Cumplimiento.

Dentro de cada sección, se especifican los objetivos de los distintos controles para la seguridad de la información. Para cada uno de los controles se indica, asimismo, una guía para su implantación.

3.2.8. PDCA (Planear-Hacer-Verificar-Actuar):

La implantación de un Sistema de Gestión de Seguridad de la Información es una decisión estratégica que debe involucrar a toda la organización y que debe ser apoyada y dirigida desde la dirección. El modelo de proceso PDCA, un modelo dividido en cuatro fases en el que finalizada la última y analizados sus resultados se vuelve a comenzar de nuevo la primera. Las siglas PDC corresponden en inglés a **Plan, Do, Check, Act** y han sido traducidas como Planificación, Ejecución, Seguimiento y Mejora.

La primera fase del Modelo PDCA para la implantación del sistema es la fase de **Planificación.**

Durante esta fase se realiza un estudio de la situación de la organización desde el punto de vista de la seguridad, para estimar las medidas que se van a implantar en función de las necesidades detectadas. No toda la información de la que disponemos tiene el mismo valor o está sometida a los mismos riesgos. Por ello, es importante realizar un Análisis de Riesgos que valore los activos de información y vulnerabilidades a las que están expuestas. Así mismo, es necesaria una Gestión de dichos riesgos para reducirlos en la medida de lo posible.

Con el resultado obtenido en el Análisis y la Gestión de Riesgos estableceremos unos controles adecuados que nos permitan minimizar los riesgos.

En la fase de Ejecución del Modelo PDCA se lleva a cabo la implantación de los controles de seguridad seleccionados en la fase anterior. Estos controles se refieren a los controles más técnicos, así como a la documentación necesaria.

Esta fase también requiere un tiempo de concienciación y formación para dar a conocer qué se está haciendo y por qué, al personal de la empresa.
La tercera fase de nuestro Modelo PDCA es la fase de Seguimiento. En ella se evalúa la eficacia y el éxito de los controles implantados. Por ello, es muy importante contar con registros e indicadores que provengan de estos controles.

El Modelo PDCA se completa con la fase de Mejora durante la que se llevarán a cabo las labores de mantenimiento del sistema. Si durante la fase anterior de Seguimiento se ha detectado algún punto débil, este es el momento de mejorarlo o corregirlo. Para ello se cuenta con tres tipos de medidas: medidas correctoras, medidas preventivas y medidas de mejora.

Al finalizar las cuatros fases, se toman los resultados de la última y se comienza nuevamente la primera. Si el objetivo de la implantación de este sistema era la certificación, el ciclo completo tendrá una duración de un año, coincidiendo con las realizaciones de las auditorias de certificación que Se realizan cada año.

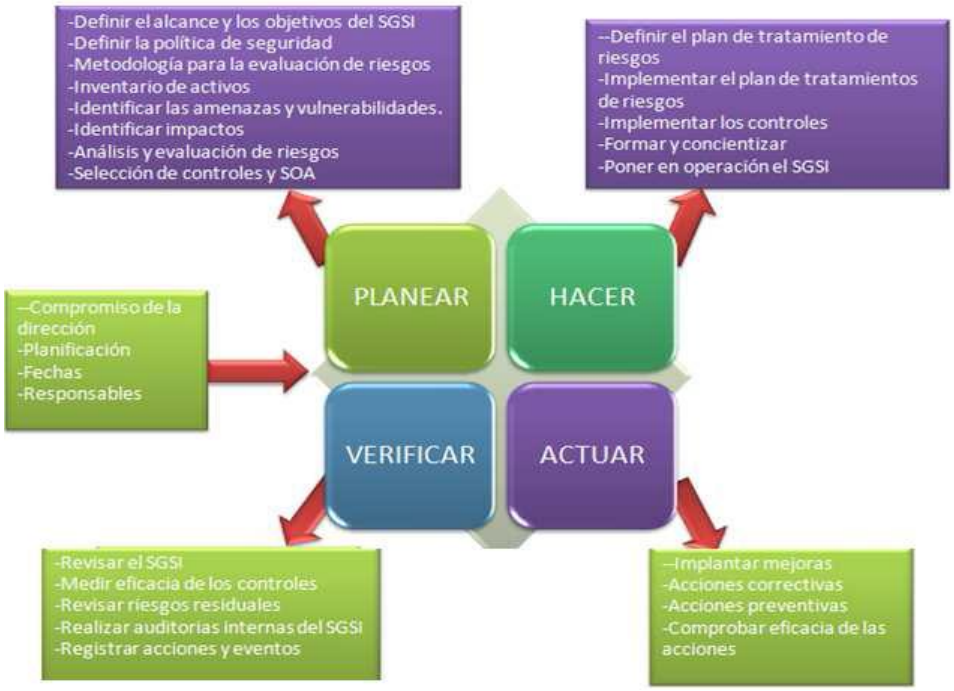

Ilustración 1 Ciclo PHVA para el SGSI.
Fuente:http://www.iso27000.es/sgsi.html#section2d.

3.2.8.1 PLANIFICACIÓN

Ilustración 2 Fase de Planificación

- Definir alcance del SGSI: en función de características del negocio, organización, localización, activos y tecnología, los límites del SGSI. El SGSI no tiene por qué abarcar toda la organización; de hecho, es recomendable empezar por un alcance limitado.
- Definir política de seguridad: que incluya el marco general y los objetivos de seguridad de la información de la organización, tenga en cuenta los requisitos de negocio, legales y contractuales en cuanto a seguridad.
- Definir el enfoque de evaluación de riesgos: definir una metodología de evaluación de riesgos apropiada para el SGSI y las necesidades de la organización, desarrollar criterios de aceptación de riesgos y determinar el nivel de riesgo aceptable.
- Inventario de activos: todos aquellos activos de información que tienen algún valor para la organización y que quedan dentro del alcance del SGSI.
- Identificar amenazas y vulnerabilidades: todas las que afectan a los activos del inventario.
- Identificar los impactos: los que podría suponer una pérdida de la confidencialidad, la integridad o la disponibilidad de cada uno de los activos.
- Análisis y evaluación de los riesgos: evaluar el daño resultante de un fallo de seguridad y la probabilidad de ocurrencia del fallo; estimar el nivel de riesgo resultante y determinar si el riesgo es aceptable o requiere tratamiento.
- Identificar y evaluar opciones para el tratamiento del riesgo: el riesgo puede reducido, eliminado, aceptado o transferido.
- Selección de controles: seleccionar controles para el tratamiento el riesgo en función de la evaluación anterior.
- Aprobación por parte de la Dirección del riesgo residual y autorización de implantar el SGSI: hay que recordar que los riesgos de seguridad de la información son riesgos de negocio y sólo la Dirección puede tomar decisiones sobre su aceptación o tratamiento.
- Confeccionar una Declaración de Aplicabilidad: Es, en definitiva, un resumen de las decisiones tomadas en cuanto al tratamiento del riesgo.

3.2.8.1.1 ALCANCE DEL SGSI

En primera medida la organización debe establecer el alcance del Sistema de Gestión de Seguridad en la Información SGSI, el alcance está en función de las características del negocio, la organización, localización, activos y tecnología por lo que definir el alcance no implica abarcar toda la organización, es más, es recomendable empezar por un alcance limitado, en el que se involucren los procesos *core* del negocio o que contengan la información más relevante para la compañía, es decir los que se han identificado en el mapa como misionales.

Es indispensable disponer del mapa de procesos, e identificar claramente aquellos que harán parte de alcance. Tener claro las terceras partes y su influencia sobre la seguridad de la información, es importante en el momento de definir el alcance, los requisitos legales y contractuales relacionados con la seguridad de la información deben quedar contemplados también dentro del alcance del sistema.

Crear mapas de redes y sistemas, definir las ubicaciones físicas y disponer de organigramas organizativos facilita establecer con claridad el alcance del SGSI.

Para el caso de laboratorios de análisis microbiológico sugerimos que el alcance de SGSI se enfoque en los procesos misionales, típicamente definidos como:

- Solicitar toma de muestras
- Planeación de muestreos
- Realizar muestreo
- Analizar muestras
- Elaborar informe de resultados

3.2.8.2 IMPLEMENTACIÓN (HACER)

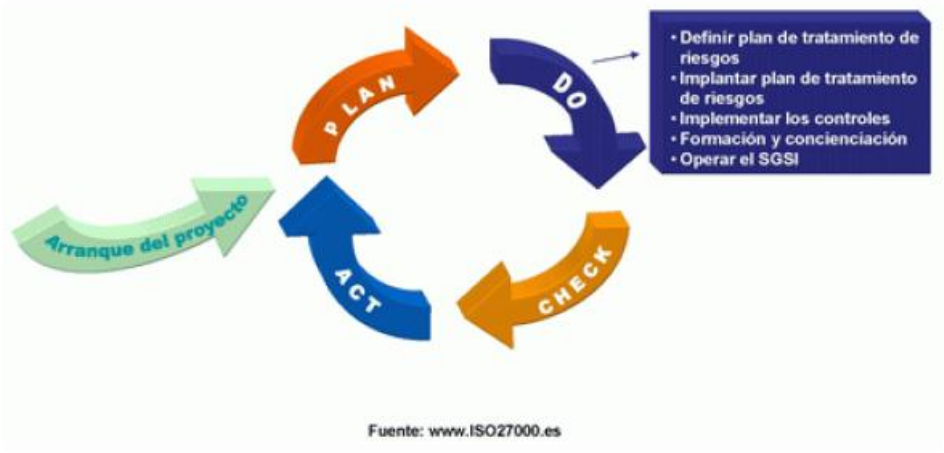

Ilustración 3 Fase Hacer

- Definir plan de tratamiento de riesgos: que identifique las acciones, recursos, responsabilidades y prioridades en la gestión de los riesgos de seguridad de la información.
- Implantar plan de tratamiento de riesgos: con la meta de alcanzar los objetivos de control identificados.
- Implementar los controles: todos los que se seleccionaron en la fase anterior.
- Formación y concienciación: de todo el personal en lo relativo a la seguridad de la información.
- Desarrollo del marco normativo necesario: normas, manuales, procedimientos e instrucciones.
- Gestionar las operaciones del SGSI y todos los recursos que se le asignen.
- Implantar procedimientos y controles de detección y respuesta a incidentes de seguridad.

3.2.8.3 SEGUIMIENTO (CHEQUEAR)

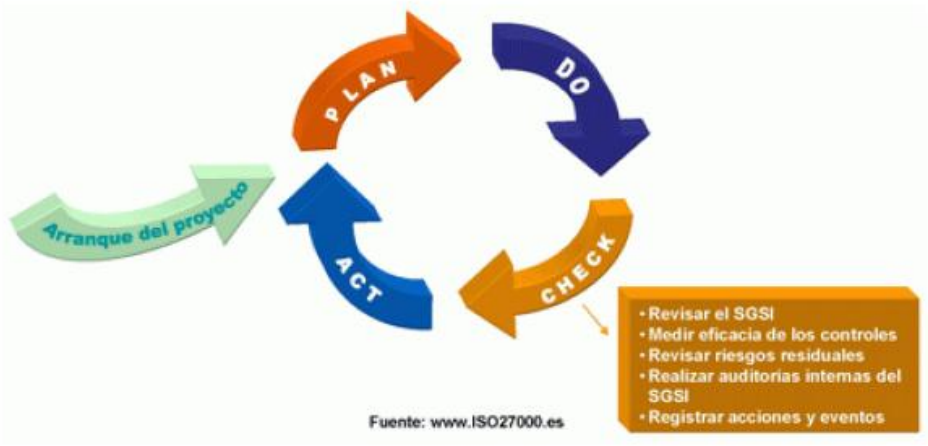

Ilustración 4 Fase Chequear

- Ejecutar procedimientos y controles de monitorización y revisión: para detectar errores en resultados de procesamiento, identificar brechas e incidentes de seguridad, y comprobar si las acciones tomadas para resolver incidentes de seguridad han sido eficaces.
- Revisar regularmente la eficacia del SGSI: en función de los resultados de auditorías de seguridad.
- Medir la eficacia de los controles.
- Revisar regularmente la evaluación de riesgos: influencian los cambios en la organización, tecnología, procesos y objetivos de negocio, amenazas, eficacia de los controles o el entorno.
- Realizar regularmente auditorías internas: para determinar si los controles, procesos y procedimientos del SGSI mantienen la conformidad con los requisitos de ISO 27001.
- Revisar regularmente el SGSI por parte de la Dirección.
- Actualizar planes de seguridad: teniendo en cuenta los resultados de la monitorización y las revisiones.
- Registrar acciones y eventos que puedan tener impacto en la eficacia o el rendimiento del SGSI.

3.2.8.4 MEJORA CONTINÚA (ACTUAR)

Ilustración 5 Fase Actuar

- Implantar mejoras: poner en marcha todas las mejoras que se hayan propuesto en la fase anterior.
- Acciones correctivas: para solucionar no conformidades detectadas.
- Acciones preventivas: para prevenir potenciales no conformidades.
- Comunicar las acciones y mejoras: a todos los interesados y con el nivel adecuado de detalle.
- Asegurarse de que las mejoras alcanzan los objetivos pretendidos: la eficacia de cualquier acción, medida o cambio debe comprobarse siempre.

3.2.9. DEFINICIÓN DE LAS POLITICAS, ORGANIZACIÓN Y ALCANCE DEL SISTEMA DE GESTIÓN

La implantación de un Sistema de Gestión de Seguridad de la Información comienza con su correcto diseño. Para ello deberemos definir cuatro aspectos fundamentales. Primero, el alcance del sistema.
Segundo, la Política de Seguridad a seguir. Tercero, la organización de la seguridad. Y cuarto, los programas de concienciación y formación del personal.

El primer paso, consiste en definir el alcance del sistema. Este debe determinar las partes o procesos de la organización que van a ser incluidos dentro del mismo.

En este momento, la empresa debe determinar cuáles son los procesos críticos para su organización decidiendo qué es lo que quiere proteger y por dónde debe empezar.

Dentro del alcance deben quedar definidas las actividades de la organización, las ubicaciones físicas que van a verse involucradas, la tecnología de la organización y las áreas que quedarán excluidas en la implantación del sistema.

Es importante que durante esta fase, se estimen los recursos económicos y de personal que se van a dedicar a implantar y mantener el sistema. De nada sirve que la organización realice un esfuerzo importante durante la implantación si después no es capaz de mantenerlo.
Tras la definición del alcance, el siguiente paso es establecer la Política de Seguridad. Su principal objetivo es recoger las directrices que debe seguir la seguridad de la información de acuerdo a las necesidades de la organización y a la legislación vigente. Además, debe establecer las pautas de actuación en el caso de incidentes y definir las responsabilidades.
El documento debe delimitar qué se tiene que proteger, de quién y por qué. Debe explicar qué es lo que está permitido y qué no; determinar los límites del comportamiento aceptable y cuál es la respuesta si estos se sobrepasan; e identificar los riesgos a los que está sometida la organización.

Para que la Política de Seguridad sea un documento de utilidad en la organización y cumpla con lo establecido en la norma UNE-ISO/IEC 27001 debe cumplir con los siguientes requisitos:

· Debe de ser redactada de una manera accesible para todo el personal de la organización. Por lo tanto debe ser corta, precisa y de fácil comprensión.
· Debe ser aprobada por la dirección y publicitada por la misma.
· Debe ser de dominio público dentro de la organización, por lo que debe estar disponible para

ILUSTRACIÓN 6 POLITICAS DEL SGSI

3.2.10. ANÁLISIS Y VALORACIÓN DE LOS RIESGOS

Antes de entrar de lleno en el análisis y valoración de los riesgos a los que deben hacer frente nuestros negocios, es importante entender algunos conceptos básicos tales como, riesgos, amenazas y vulnerabilidades, que nos van a facilitar el llevar a cabo un análisis y valoración adecuados.
La primera definición, como no puede ser de otra forma, se refiere a los riesgos.

Se considera riesgo la estimación del grado de exposición de un activo, a que una amenaza se materialice sobre él causando daños a la organización.
El riesgo indica lo que le podría pasar a los activos si no se protegen adecuadamente.
Las amenazas son los eventos que pueden desencadenar un incidente, produciendo daños materiales o inmateriales en los activos.
Las vulnerabilidades son las debilidades que tienen los activos o grupos de activos que pueden ser aprovechadas por una amenaza.

· El **impacto** es la consecuencia de la materialización de una amenaza sobre un activo.
· El **riesgo intrínseco** es la posibilidad de que se produzca un impacto determinado en un activo o en un grupo de activos.

· Las **salvaguardas** son las prácticas, procedimientos o mecanismos que reducen el riesgo. Estas pueden actuar disminuyendo el impacto o la probabilidad.
· Por último, tenemos la definición de **riesgo residual** que es el riesgo que queda tras la aplicación de salvaguardas. Por muy bien que protejamos nuestros activos, es imposible eliminar el riesgo al 100% por lo que siempre quedará un riesgo residual en el sistema que la organización deberá asumir y vigilar.

Conocer todos estos términos facilita la comprensión del tema que nos ocupa, el análisis de riesgos.
Podríamos decir que este proceso consiste en identificar los riesgos de seguridad en nuestra empresa, determinar su magnitud e identificar las áreas que requieren implantar salvaguardas.

ILUSTRACIÓN 7 AMENAZAS Y RIESGOS

ILUSTRACIÓN 8 TRATAMIENTO DEL RIESGO EN EL SGSI

3.2.11. PROCESO DE CERTIFICACIÓN

Al finalizar la implantación del Sistema de Gestión de Seguridad de la Información tenemos la opción de certificarlo, es decir, obtener un documento a través de un tercero de confianza que verifica su correcta implantación.

Con ello certificamos la gestión del sistema pero no las medidas implantadas o la seguridad de la empresa. Lo que certifica es que la empresa gestiona adecuadamente la seguridad. Las empresas certifican sus sistemas, entre otras razones, para mejorar su imagen, porque sus clientes lo demanda o porque creen que es bueno para su gestión interna.

Para poder certificarlo, nuestro Sistema de Gestión de Seguridad de la información tiene que estar basado en la norma UNE-ISO/IEC 27001. Además, debe estar implantado y funcionando y tienen que existir evidencias que lo demuestren. Así mismo, tiene que contar con recursos económicos y personal de la empresa para atender a las demandas de la entidad de certificación.

En el momento de contratar a una entidad de certificación, debemos asegurarnos de que cuenta con auditores cualificados para verificar la correcta implantación del sistema según la norma UNE-ISO/IEC 27001.

Además, deberemos comprobar que posee la adecuada acreditación que la reconoce como una entidad competente para la realización de esa actividad. La entidad de certificación debe estar acreditada para la norma en la que se desea realizar la certificación, asegurando así que cumple con los requisitos para realizar correctamente su trabajo.

Después de cada una de las fases de la auditoría la entidad de certificación emite un informe en el que se indican los resultados de la misma. En estos informes pueden aparecer los siguientes resultados:

· **Uno.** Todo correcto.

· **Dos.** Observaciones sobre el sistema que no tienen excesiva relevancia pero que deben ser tenidas en cuenta en la siguiente fase de la auditoría, bien para ser revisadas in-situ o bien para ser mejoradas en el siguiente ciclo de mejora.

· **Tres.** No conformidades menores. Estas son incidencias encontradas en la implantación subsanables mediante la presentación de un Plan de Acciones Correctivas en el que se identifica la incidencia y la manera de solucionarla.

· **Cuatro.** No conformidades mayores que deben ser subsanadas por la empresa. Sin su resolución y, en la mayor parte de los casos, la realización de una auditoría extraordinaria por parte de la entidad de certificación, no se obtendría el certificado ya que se trata de incumplimientos graves de la norma

En caso de darse tras la auditoría documental es necesario su resolución antes de llevar a cabo la auditoría in-situ. Una vez conseguido el certificado del sistema, éste tiene una validez de tres años, aunque está sujeto a revisiones anuales.

IV. CONCLUSIONES

- La implementación de un SGSI en una organización es de gran utilidad al proporcionar una metodología adecuada para garantizar la confidencialidad, la integridad y la disponibilidad de los activos de su negocio que tengan que ver con la información.

- Tan importante como los procesos y procedimientos es el diseño de una organización que pueda desarrollar todas las actividades del negocio en la línea con lo indicado en el SGSI para lo cual es importante que la organización sea transversal y su enfoque sea por procesos.

- Es fundamental la concreción de los controles de seguridad para supervisar el seguimiento de los planes de acción, los controles incluidos, concretos y medibles en el tiempo permiten evaluar la efectividad de los planes en acción.

- El SGSI tiene que ser dinámico y fácilmente adaptable a los cambios y las mejoras a introducir en la compañía, la aplicación del modelo PHVA (Planear, Hacer, Verificar, Actuar) es fundamental, basado en el concepto de mejora continúa, la competencia en su manejo es de gran utilidad en contexto de un SGSI. El enfoque sistémico propuesto por la norma ISO/IEC 27001 permitirá las siguientes consecuencias:

  - La toma de decisiones sobre la seguridad de los activos críticos de información se basa en información a priori (análisis de riesgos) y a posteriori (auditorías e indicadores).
  - Se orienta a la mejora continua, a través de la gestión de acciones correctivas y preventivas.
  - Si se decide obtener la certificación ISO/IEC 27001 del sistema, mejora la imagen del organismo y se contribuye a generar confianza entre los usuarios y la empresa.

V. RECOMENDACIONES

Para que la implementación de un modelo SGSI sea exitosa debemos tener en cuenta lo siguiente:

- Asegurarse de que se establezcan objetivos y planes del SGSI en la organización.
- Establecer roles y responsabilidades de la seguridad de la información.
- Comunicar a la organización la importancia de lograr los objetivos de seguridad de la información y de cumplir con la política de seguridad, como de sus responsabilidades legales, contractuales y la necesidad de mejora continua.
- Asignar suficiente recursos al modelo SGSI en todas sus fases
- Decidir los criterios de aceptación de riesgos y sus correspondientes niveles.
- Realizar revisiones periódicas al modelo SGSI.
- Determinar las competencias necesarias para el personal que realiza tareas en la implementación del modelo SGSI.
- Evaluar la eficacia de las acciones realizadas
- Actualizar la evaluación de los riesgos y del plan de tratamiento de riesgos.
- Disponer de un enfoque y un marco de trabajo para implementar, mantener, monitorear y mejorar la seguridad de la información, que sean consistentes con la cultura de la organización.
- Asegurar un buen entendimiento de los requisitos de seguridad de la información apoyándose en metodologías para gestión de riesgos.
- Aplicar correctamente todos los controles implementados, manteniendo de esa forma la seguridad adecuada.

VI. REFERENCIAS BIBLIOGRÁFICAS

- Metodología de Implantación de un SGSI en grupos empresariales de relación jerárquica – Gustavo Pallas y María Eugenia Corti. http://www.criptored.upm.es/cibsi/cibsi2009/docs/Papers/CIBSI-Dia2-Sesion3(4).pdf

- Implementación efectiva de un SGSI ISO 27001. **Rodrigo Baldecchi. 2014.** http://www.isaca.org/chapters8/Montevideo/cigras/Documents/CIGRAS2014%20-%20Exposici%C3%B3n%202%20CIGRAS%20ISO%2027001%20-%20rbq.pdf

- Diseño de una Metodología para la implementación del sistema de gestión de seguridad de la información – SGSI, basado en ISO 27001. Johanna carolina Buitrago estrada, Diego Hernando Bonilla Pineda, Carol Estefanie Murillo Varon. **Bogota – 2012.**

  http://repository.ean.edu.co/bitstream/handle/10882/2692/MurilloCarol2012.pdf?sequence=1

- Implantación de un SGSI en la empresa. Instituto Nacional de Tecnologías de la Comunicación. **España.** https://www.incibe.es/extfrontinteco/img/File/intecocert/sgsi/img/Guia_apoyo_SGSI.pdf

- "Guía Metodológica implantación de un SGSI". **AGESIC – 2012.** http://documentslide.com/documents/guia-metodologica-sgsi.html

- "Metodologías para la implantación de un SGSI". **Maria Eugenia Corti – 2010** https://www.agesic.gub.uy/innovaportal/file/1065/1/primera.pdf