1.1. ¿QUÉ ES UN SGSI?

Las siglas SGSI son el acrónimo de Sistema de Gestión de Seguridad de la Información.

Antes de avanzar en la auditoría de un SGSI, es necesario dejar claro qué entendemos por un SGSI y para ello debemos definir el significado de ciertos términos en los que habitualmente suele haber cierta discrepancia.

Según el diccionario de la Real Academia Española, un sistema es un *"conjunto de cosas que relacionadas entre sí ordenadamente contribuyen a determinado objeto"* y como estamos hablando de un sistema de gestión *"conjunto de cosas que relacionadas entre sí ordenadamente contribuyen a gestionar y administrar una Organización".*

Si consultamos las definiciones que figuran en la norma ISO 9000, *Sistemas de gestión de la calidad. Fundamentos y vocabulario,* un sistema de gestión es un *"sistema para establecer la política y los objetivos y para lograr dichos objetivos",* entendiendo por sistema un *"conjunto de elementos mutuamente relacionados o que interactúan".*

Por otra parte, el modelo de excelencia EFQM, de la Fundación Europea para la Gestión de Calidad, define un sistema de gestión como un *"Esquema general de procesos y procedimientos que se emplea para garantizar que la Organización realiza todas las tareas necesarias para alcanzar sus objetivos".*

En resumen, un sistema de gestión no es otra cosa, que el marco de funcionamiento de una Organización en el que se integran tanto la misión, visión, valores, objetivos principales y secundarios de la misma, como las políticas, procedimientos, registros e indicadores, que dan forma al sistema. Disponer del marco de trabajo que proporciona un sistema de gestión le permite a una Organización incrementar la eficacia y eficiencia de sus procesos.

Para desarrollar e implementar el sistema de gestión de una Organización, es necesario realizar las siguientes actividades y tareas:

- Determinar las necesidades y expectativas de todas las partes interesadas.
- Establecer la política y objetivos de la Organización.
- Determinar los procesos y las responsabilidades necesarias para alcanzar sus objetivos de negocio.
- Determinar y proporcionar los recursos necesarios para alcanzar sus objetivos de negocio.
- Establecer los métodos para medir la eficacia y eficiencia de cada proceso.
- Aplicar estas medidas para determinar la eficacia y eficiencia de cada proceso.
- Determinar los medios para prevenir las no conformidades y eliminar sus causas.
- Establecer y aplicar un proceso para la mejora continua del sistema de gestión.

Una Organización que adopta un modelo de gestión adecuado genera confianza en la capacidad de sus procesos, y lo que es lo mismo, genera confianza en que la Organización será capaz de alcanzar sus objetivos, proporcionándole igualmente una base para la mejora continua, lo que es un paso muy importante para mejorar el grado de satisfacción de todas las partes interesadas y facilita el éxito de la Organización.

Para que una Organización sea eficiente necesita disponer de un sistema de gestión, y para ello la alta dirección debe, por medio de su liderazgo y sus acciones, crear un ambiente de trabajo en el cual todo el personal de la Organización se encuentre completamente involucrado y en el que el sistema de gestión suponga una mejora continua de los procesos de la Organización aumentando su eficiencia y eficacia. Para ello la alta dirección debe:

- Establecer y mantener la política y los objetivos la Organización.
- Promover la política y los objetivos de la Organización a todos los niveles de su estructura para aumentar la concienciación, la motivación y la participación de todo el personal.
- Asegurarse de que la Organización trabaja con un enfoque de cumplimiento de requisitos.
- Asegurarse de que se implementan los procesos apropiados para cumplir con los requisitos de todas las partes interesadas y para alcanzar los objetivos de Organización.

- Asegurarse de que se ha establecido, implementado y se mantiene un sistema de gestión eficaz y eficiente que permite alcanzar los objetivos de la Organización.
- Asegurarse de que están disponibles los recursos necesarios.
- Revisar periódicamente el sistema de gestión.
- Tomar decisiones sobre las acciones a tomar en relación con la política y con los objetivos de la calidad.
- Tomar decisiones sobre las acciones a tomar en relación con la mejora del sistema de gestión.

El objetivo de la mejora continua del sistema de gestión de la Organización es aumentar la eficacia y eficiencia de los procesos de la misma, lo que implica el aumento de la satisfacción de todas las partes interesadas. Para ello es necesario realizar una serie de actividades como:

- El análisis y la evaluación de la situación existente para identificar las áreas para la mejora.
- El establecimiento de los objetivos para la mejora.
- La búsqueda de posibles soluciones para alcanzar los objetivos.
- La evaluación de dichas soluciones y su selección.
- La implementación de la solución seleccionada.
- La medición, verificación, análisis y evaluación de los resultados de la implementación para determinar que se han alcanzado los objetivos.
- La formalización de los cambios.

La mejora es una actividad continua, por ello es necesario revisar la información que proporciona el sistema de gestión para determinar oportunidades de mejora. También se debe utilizar la información proveniente de las partes interesadas, de las auditorías, y de la revisión del sistema de gestión para identificar otras oportunidades adicionales para la mejora.

Como resumen, al implantar un SGSI se busca gestionar la seguridad de la información de una Organización bajo un modelo basado en la mejora

continua, donde la Organización que decide implementarlo adopta un enfoque por procesos para la creación, implementación, operación, supervisión, revisión y mantenimiento de la seguridad de su información.

1.2. CICLO BÁSICO DE IMPLANTACIÓN DE UN SGSI

Los Sistemas de Gestión de la Seguridad de la Información desarrollados según la norma ISO 27001, igual que muchos otros sistemas de gestión, se basan, como se ha indicado anteriormente, en el concepto de mejora continua.

El "círculo de Deming" (de Edwards Deming), también conocido como modelo o ciclo PDCA es una estrategia de mejora continua de la calidad en cuatro fases, basada en un concepto ideado por Walter A. Shewhart.

Las siglas PDCA son el acrónimo de Plan, Do, Check, Act (Planificar, Hacer, Comprobar, Actuar).

A continuación, se describen las **fases** de este ciclo de mejora continua, nombre con el que también se le conoce al ciclo PDCA, que como se puede comprobar son de aplicación a cualquier proyecto de mejora de procesos sean del tipo que sean.

PLANIFICAR

- Identificar el proceso que se quiere mejorar.
- Recopilar datos para profundizar en el conocimiento del proceso.
- Analizar e interpretar los datos.
- Establecer los objetivos de mejora.
- Detallar las especificaciones de los resultados esperados.
- Definir los procesos necesarios para conseguir estos objetivos, verificando las especificaciones.

HACER

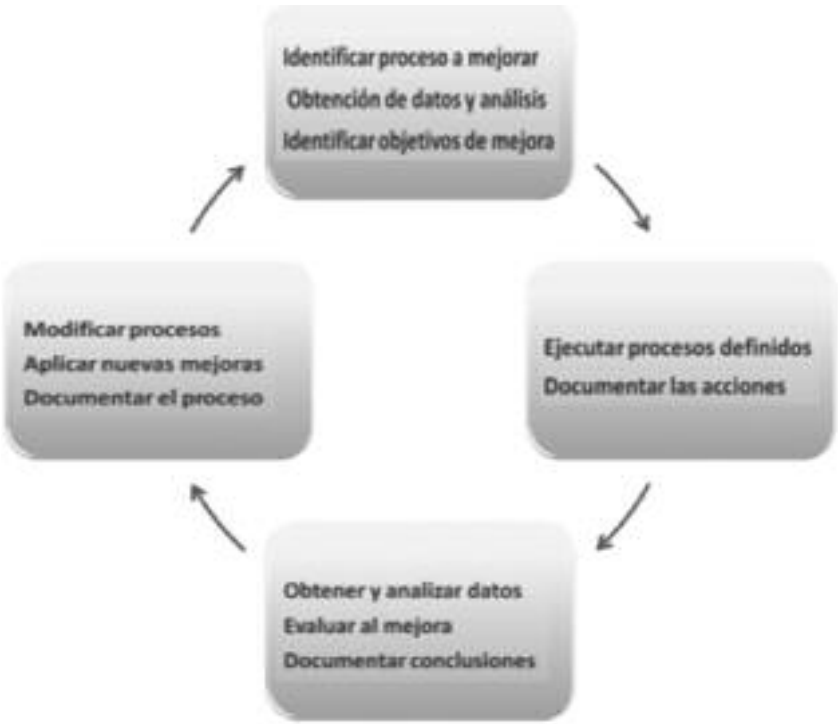
- Ejecutar los procesos definidos en el paso anterior.
- Documentar las acciones realizadas.

COMPROBAR

- Pasado un periodo de tiempo previsto de antemano, volver a recopilar datos de control y analizarlos, comparándolos con los objetivos y especificaciones iniciales, para evaluar si se ha producido la mejora esperada.
- Documentar las conclusiones.

ACTUAR

- Modificar los procesos según las conclusiones del paso anterior para alcanzar los objetivos con las especificaciones iniciales, si fuese necesario.
- Aplicar nuevas mejoras, si se han detectado errores en el paso anterior.
- Documentar el proceso.



A continuación vemos las **tareas** que se realizan en cada una de fases del ciclo PDCA en el caso de un Sistema de Gestión de Seguridad de la Información:

PLANIFICAR

- 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.
- Realización de un Análisis de Riesgos que ofrezca una valoración de los activos de información y las vulnerabilidades a las que están expuestos.
- Elaboración del plan de gestión de riesgos.

HACER

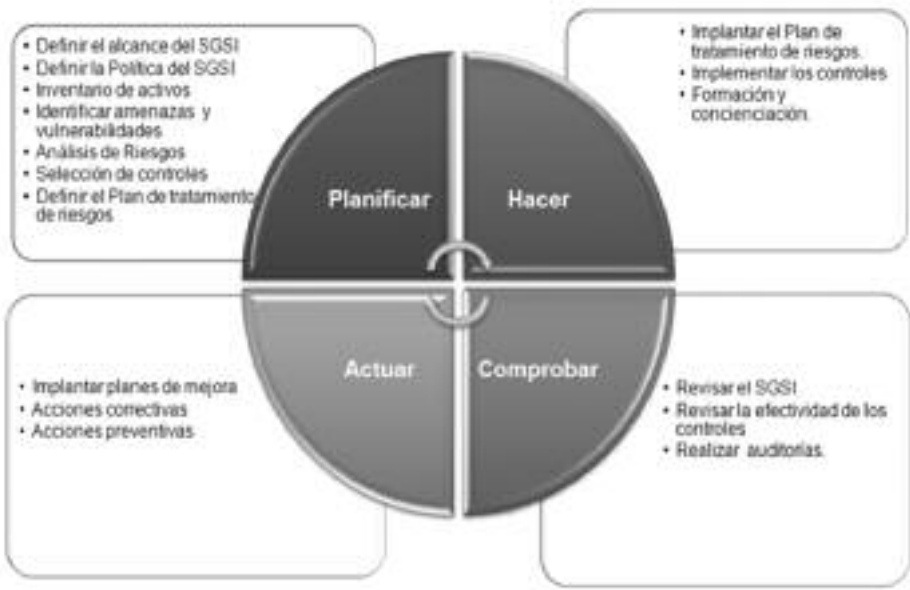
- Ejecución del plan de acción e implantación de los controles.
- Revisión de la documentación (políticas, procedimientos, instrucciones y registros).
- Concienciación y formación.

COMPROBAR

- Evaluación de la eficacia y eficiencia de los controles implantados.
- Verificación de registros e indicadores.
- Verificación del correcto funcionamiento del SGSI.

ACTUAR

- Mantenimiento del sistema.
- Realización de tareas de mejora y de corrección.



Como resumen de lo anterior, **Planificar** se refiere a la creación: comprender los requisitos de seguridad de la información de una Organización y la necesidad de establecer una política de seguridad de la información y sus objetivos. **Hacer** se refiere a la implementación y operación de los controles para gestionar los riesgos de seguridad de la información de una Organización en el marco de sus riesgos empresariales generales. **Comprobar** se refiere a la supervisión y revisión el rendimiento y la eficacia del SGSI, y **Actuar** se refiere al aseguramiento de la mejora continua sobre la base de la medición objetiva.

En definitiva, con un SGSI, la Organización lo que busca es conocer y gestionar riesgos a los que está expuesta la información de la Organización, lo que le permitirá gestionar la seguridad y actuar mediante una sistemática definida, documentada y conocida por todos, que se revisa y mejora en cada vuelta del ciclo PCDA.

La seguridad al 100% no existe, por lo que garantizar un nivel de protección total es imposible, incluso en el hipotético caso de que la Organización que decidiera implantarlo dispusiera de un presupuesto ilimitado. Por lo tanto, el propósito de un SGSI no es garantizar que una Organización es segura, si no que esta gestiona la seguridad y garantiza, eso sí, que los riesgos de la seguridad de la información sean conocidos, gestionados y tratados en base a los criterios definidos por la propia Organización de acuerdo a su estrategia de seguridad. Todo este proceso de gestión debe realizarse de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías. Además de esto, se deben dejar evidencias de las acciones y que se pueda realizar una trazabilidad clara.

1.3. BENEFICIOS DE UN SGSI

Para entender el sentido o la motivación de la implantación de un sistema de gestión de seguridad de la información, hay que tener en cuenta

que el origen de una gestión inadecuada de la seguridad puede estar en una o varias de las siguientes **causas**:

- Errores humanos.
- Acciones malintencionadas.
- Falta de control.
- Fallo de los sistemas.
- Carencia de formación y concienciación.
- Incidentes externos.
- Incumplimiento legal.

Estas causas pueden desembocar en una serie de graves **consecuencias,** entre las que se encuentran:

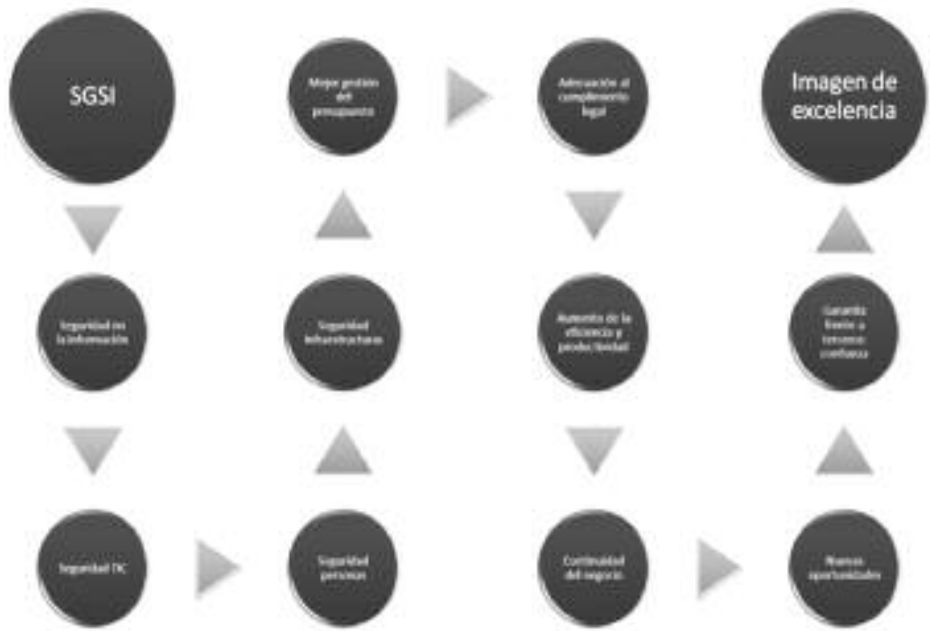
- Pérdida documental.
- Pérdida de confidencialidad.
- Indisponibilidad de la información.
- Alto tiempo de recuperación.
- Baja productividad.
- Aumento de los costes.
- Disminución del nivel de servicio.
- Pérdida reputacional.
- Pérdida de oportunidades de negocio.
- Pérdida de clientes.

La implantación de un sistema de gestión de seguridad de la información, proporciona una serie de beneficios y puede considerarse como una buena alternativa a tener en cuenta para que una Organización pueda establecer una metodología y una serie de medidas con las que ordenar, sintetizar y simplificar de manera continua el esfuerzo que ya realiza o que debería realizar para garantizar la seguridad de su información. Esta mejora en el nivel de seguridad se verá reflejada en una serie de **ventajas** que se describen a continuación:

- Reducción de riesgos
  Esto se consigue realizando un análisis de riesgos, y elaborando un conjunto de planes de acción derivado del mismo, que contemplará la implementación de un conjunto de salvaguardas, lo que reducirá los riesgos hasta el nivel asumible por la Organización, este proceso estará alineado los objetivos de negocio de esta.
- Aumento del retorno sobre la inversión en seguridad (ROSI)
  La implantación de un SGSI permite una optimización de recursos y un incremento de la eficacia y eficiencia en el empleo de los mismos, lo que supone una mejora en el retorno de la inversión. Además de que la toma de decisiones podrá estar basada en prioridades y datos cuantitativos, no sólo cualitativos, lo que permite gestionar mejor la inversión en seguridad, evitándose gastos innecesarios, inesperados, y sobredimensionados.
- Aumenta la madurez en la gestión de la seguridad
  La implementación de un SGSI transforma la seguridad en una actividad de gestión, como cualquier otro proceso de la Organización. Este concepto es importante dado que la seguridad deja de ser un conjunto de actividades técnicas organizadas, para transformarse en un proceso con un ciclo de vida metódico y controlado. De este modo va aumentando el nivel de madurez de la Organización en cuanto a la seguridad y mejorando en cada vuelta de ciclo.
- Cumplimiento legal
  Durante la implementación de un SGSI se evalúa el cumplimiento de la legislación vigente y se verifica la adecuación y el cumplimiento. Por lo tanto, se crea un marco legal en evaluación continua.
- Generación de valor y factor diferenciador
  Es en un importante factor diferenciador con la competencia, por las ventajas derivadas de la mejora de la imagen y de otras ventajas competitivas en el mercado.

Entre estas ventajas competitivas podemos citar las siguientes:

- Aumento de la seguridad de:
  - La información.
  - Los sistemas de información.
  - Las tecnologías de la información y las comunicaciones.
  - Las personas.
  - Las infraestructuras.
- Mejor gestión del presupuesto.
- Adecuación al cumplimiento legal (LOPD, LSSI...).
- Aumento de la eficiencia y productividad.
- Permite la continuidad del negocio.
- Nuevas oportunidades de negocio.
- Garantía frente a terceros: confianza.
- Imagen de excelencia.



CAPÍTULO 2.

CONCEPTOS GENERALES DE AUDITORÍA DE TECNOLOGÍAS DE LA INFORMACIÓN

2.1. INTRODUCCIÓN

La primera cuestión es determinar a qué nos referimos cuando hablamos de auditoría, las definiciones de auditoría que nos encontramos tienen pequeñas diferencias dependiendo del autor y área de aplicación.

"Proceso sistemático para evaluar y obtener de manera objetiva las evidencias relacionadas con informes sobre actividades económicas y otros acontecimientos relacionados".

"Es una actividad que consiste en la emisión de una opinión profesional sobre si el objeto sometido a análisis presenta adecuadamente la realidad que pretende reflejar y/o cumple las condiciones que le han sido prescritas".

"Proceso sistemático, independiente y documentado para obtener evidencias y evaluarlas de manera objetiva con el fin de determinar si cumplen con las disposiciones previamente establecidas, y si estas disposiciones se han aplicado efectivamente y son adecuadas para alcanzar los objetivos".

"Se entiende por Auditoría Informática una serie de exámenes periódicos o esporádicos de un sistema informático cuya finalidad es analizar y evaluar la planificación, el control, la eficacia, la seguridad, la economía y la adecuación de la infraestructura informática de la empresa".

"La Auditoría Informática comprende la revisión y la evaluación independiente y objetiva, por parte de personas independientes y teóricamente competentes del entorno informático de una entidad, abarcando todo o algunas de sus áreas, los estándares y procedimientos en vigor, su idoneidad y el cumplimiento de estos, de los objetivos fijados, los contratos y las normas legales aplicables, el grado de satisfacción de usuarios y directivos, los controles existentes y el análisis de riesgos".

"Proceso sistemático, independiente y documentado para obtener evidencias de la auditoría y evaluarlas de manera objetiva con el fin de determinar el grado en que se cumplen los criterios de auditoría".

2.2. GENERALIDADES

Al comenzar una auditoría, hay que establecer una serie de criterios que se van a aplicar durante la misma:

- Ámbito: es la definición que determina los límites de la auditoría e identifica los elementos, procesos, servicios y/o actividades que van a auditarse. La definición del ámbito de auditoría sirve además para hacer un uso más eficiente de los recursos que van a utilizarse durante la auditoría, incluyendo el tiempo que debe estar disponible las personas implicadas en la auditoría.
- Proceso revisión: proceso mediante el cual el equipo auditor obtiene evidencias del cumplimiento o incumplimiento de la norma auditada.
- Proyecto: es un proceso único consistente en un conjunto de actividades coordinadas y controladas con fechas de inicio y de finalización, llevadas a cabo para conseguir un objetivo conforme con requisitos específicos, incluyendo las limitaciones de tiempo, costes y recursos.
- Cumplimiento: se refiere a la conformidad de los requisitos de la norma auditada.
- Objetivos de negocio: objetivos estratégicos.
- Opinión: juicio del auditor basado en las evidencias obtenidas y analizadas.
- Informe de auditoría: producto final del proyecto de auditoría, es la herramienta utilizada por el auditor para informar de sus hallazgos, conclusiones y recomendaciones.
- Auditor: persona que lleva a cabo una auditoría.
- Equipo auditor: uno o más auditores que llevan a cabo una auditoría, con el apoyo, si es necesario, de expertos técnicos[1].
- Cliente de auditoría: organización o persona que solicita una auditoría.
- Organización auditada: organización que es auditada.

[1] Durante el libro nos referiremos al Equipo auditor independientemente de si la auditoría se planifica con una o más personas.