ISO 27001 SEGURIDAD DE LA INFORMACIÓN

ISO 27001 GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

¿Por qué ISO 27001? Porque para el fin de preservar la información, se ha demostrado que no es suficiente la implantación de controles y procedimientos de seguridad realizados frecuentemente sin un criterio común establecido, en torno a la compra de productos técnicos y sin **considerar toda la información esencial que se debe proteger.**

La Organización Internacional de Estandarización (ISO), a través de las normas recogidas en **ISO / IEC 27000**, establece una implementación efectiva de la seguridad de la información empresarial desarrolladas en las normas **ISO 27001 / ISO 27002.**

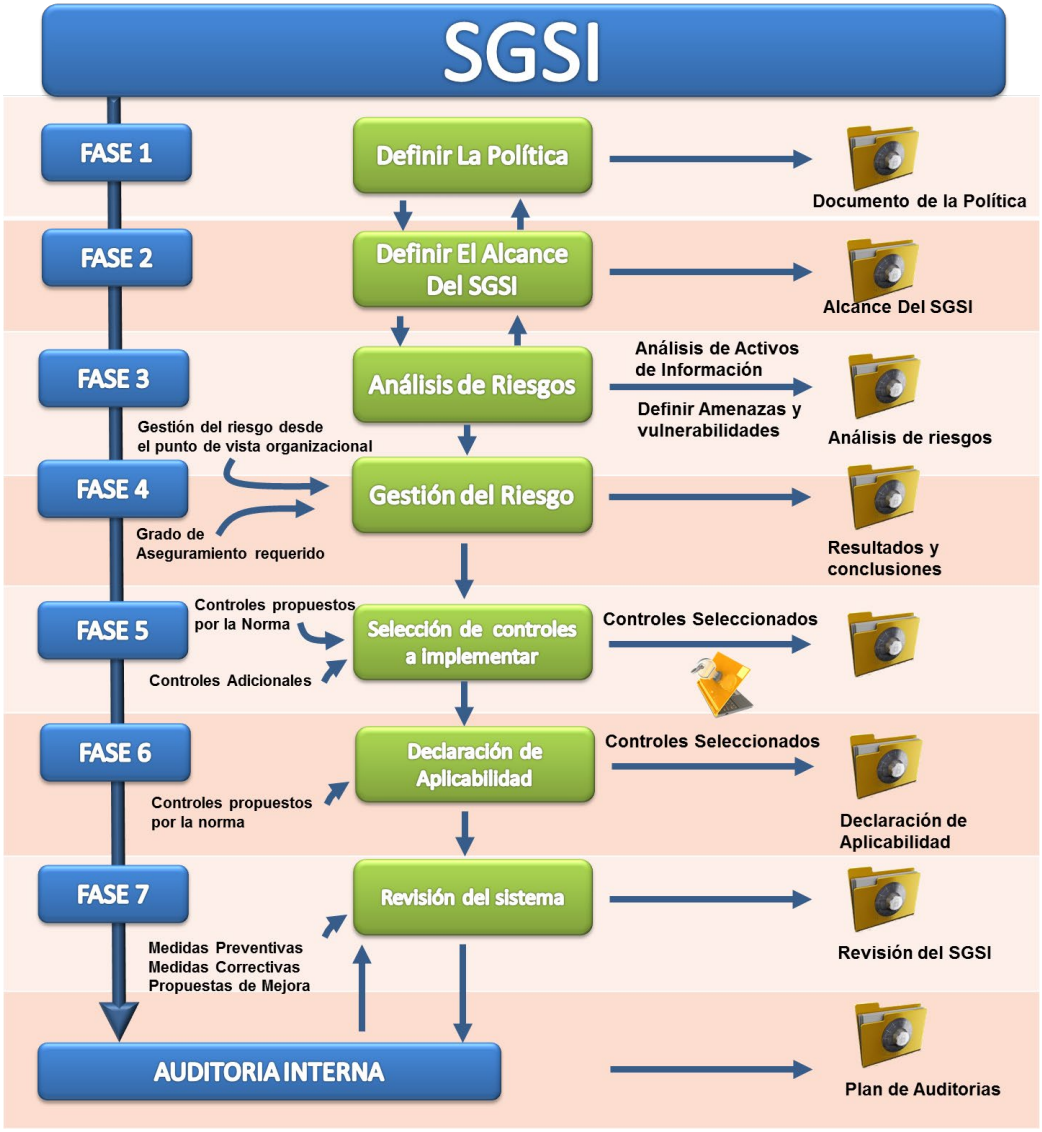
Los requisitos de la Norma **ISO 27001** norma nos aportan un **S**istema de **G**estión de la **S**eguridad de la **I**nformación **(SGSI)**, consistente en medidas orientadas a **proteger la información**, indistintamente del formato de la misma, contra cualquier amenaza, de forma que garanticemos en todo momento la continuidad de las actividades de la empresa.

Los Objetivos del SGSI son preservar la:

- **Confidencialidad**
- **Integridad**
- y **Disponibilidad** de la Información

ELEMENTOS O FASES PARA LA IMPLEMENTACIÓN DE UN SGSI

El Sistema de Gestión de La Seguridad de la Información que propone la Norma ISO 27001 se puede resumir en las siguientes fases que se detallan en la figura:



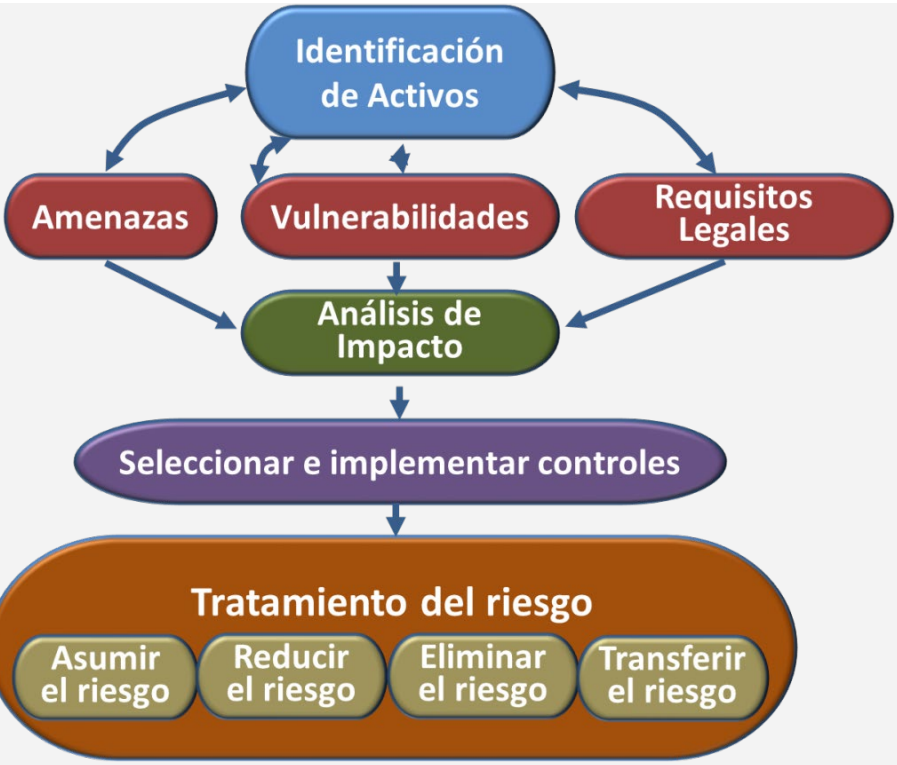
¿EN QUE CONSISTE LA EVALUACIÓN DE RIESGOS?

IMPLANTANDO LA NORMA ISO 27001

A la hora de implantar un Sistema de Gestión de la Seguridad de la Información (SGSI) según la norma **ISO 27001**, debemos considerar como eje central de este sistema **la Evaluación de Riesgos.** Este capítulo de la Norma, permitirá a la dirección de la empresa tener la visión necesaria para definir el alcance y ámbito de aplicación de la norma, así como las políticas y medidas a implantar, integrando este sistema en la metodología de mejora continua, común para todas las normas ISO.

Lo primero, es elegir una metodología de evaluación del riesgo apropiada para los requerimientos del negocio. Existen numerosas metodologías estandarizadas de evaluación de riesgos. Aquí explicaremos la metodología sugerida en la Norma.

Las fases de esta metodología son los siguientes:



Método de Evaluación y Tratamiento del Riesgo

- **1.-** Identificar los **Activos de Información** y sus responsables, entendiendo por activo todo aquello que tiene valor para la organización, incluyendo soportes físicos (edificios o equipamientos), intelectuales o informativas (Ideas, aplicaciones, proyectos ...) así como la marca, la reputación etc.
- **2.-** Identificar las **Vulnerabilidades** de cada activo: aquellas debilidades propias del activo que lo hacen susceptible de sufrir ataques o daños.

- **3.**- Identificar las **amenazas:** Aquellas cosas que puedan suceder y dañar el activo de la información, tales como desastres naturales, incendios o ataques de virus, espionaje etc.
- **4.-** Identificar los **requisitos legales** y contractuales que la organización está obligada a cumplir con sus clientes, socios o proveedores.
- **5.- Identificar los riesgos:** Definir para cada activo, la probabilidad de que las amenazas o las vulnerabilidades propias del activo puedan causar un daño total o parcial al activo de la información, en relación a su disponibilidad, confidencialidad e integridad del mismo.
- **6.- Cálculo del riesgo:** Este se realiza a partir de la probabilidad de ocurrencia del riesgo y el impacto que este tiene sobre la organización (Riesgo = impacto x probabilidad de la amenaza). Con este procedimiento determinamos los riesgos que deben ser controlados con prioridad.
- **7.- Plan de tratamiento del riesgo:** En este punto estamos preparados para definir la política de tratamiento de los riesgos en función de los puntos anteriores y de la política definida por la dirección. En este punto, es donde seleccionaremos los controles adecuados para cada riesgo, los cuales irán orientados a :
    - Asumir el riesgo
    - Reducir el riesgo
    - Eliminar el riesgo
    - Transferir el riesgo

¿QUÉ NOS APORTA LA ISO 27001?

BENEFICIOS DE LA NORMA ISO 27001

Los riesgos de seguridad de la información representan una amenaza considerable para las empresas debido a la posibilidad de pérdida financiera o daño, la pérdida de los servicios esenciales de red, o de la reputación y confianza de los clientes.

La gestión de riesgos es uno de los elementos clave en la prevención del fraude online, robo de identidad, daños a los sitios Web, la pérdida de los datos personales y muchos otros incidentes de seguridad de la información. Sin un marco de gestión de riesgos sólida, las organizaciones se exponen a muchos tipos de amenazas informáticas.

La nueva norma internacional **ISO / IEC 27001** - seguridad de la información, ayudará a las organizaciones de todo tipo para mejorar la gestión de sus riesgos de seguridad de la información.

Hoy en día, seguridad de la información está constantemente en las noticias con el robo de identidad, las infracciones en las empresas los registros financieros y las amenazas de terrorismo cibernético. Un sistema de gestión de seguridad de la información **(SGSI)** es un enfoque sistemático para la gestión de la información confidencial de la empresa para que siga siendo seguro. Abarca las personas, procesos y sistemas de TI.

El diseño y la implementación de un SGSI **(ISO / IEC 27001:2005)** dará confianza a clientes y proveedores que la seguridad de la información se toma en serio dentro de la organización, estando a la vanguardia en la aplicación de la técnica de procesos para hacer frente a las amenazas de la información y a y los problemas de la seguridad.

¿ISO 27001 ES ALGO MÁS QUE SEGURIDAD INFORMÁTICA?

¿QUÉ ENTENDEMOS POR INFORMACIÓN EN ISO 27001?

Sin duda, gran parte de la Información de una empresa se encuentra en los sistemas informáticos, sin embargo, la Norma ISO 27001 define la información como:

La información es un activo que, como otros activos importantes del negocio, tiene valor para la organización y requiere en consecuencia una protección adecuada ...
... a información adopta diversas formas. Puede estar impresa o escrita en papel, almacenada electrónicamente, transmitida por correo o por medios electrónicos, mostrada en video o hablada en conversación. Debería protegerse adecuadamente cualquiera que sea la forma que tome o los medios por los que se comparta o almacene.

Atendiendo a este concepto, ISO 27001 propone un marco de gestión de la seguridad de toda la información de la empresa, incluso si es información perteneciente al propio conocimiento y experiencia de las personas o sea tratada en reuniones etc. En este sentido las propias personas pueden ser tratadas en el SGSI como activos de información si así se cree conveniente.

Por tanto, no debemos centrar la atención solamente en los sistemas informáticos por mucho que tengan hoy en día una importancia más que relevante en el tratamiento de la información ya que de otra forma, podríamos dejar sin proteger información que puede ser esencial para la actividad de la empresa.