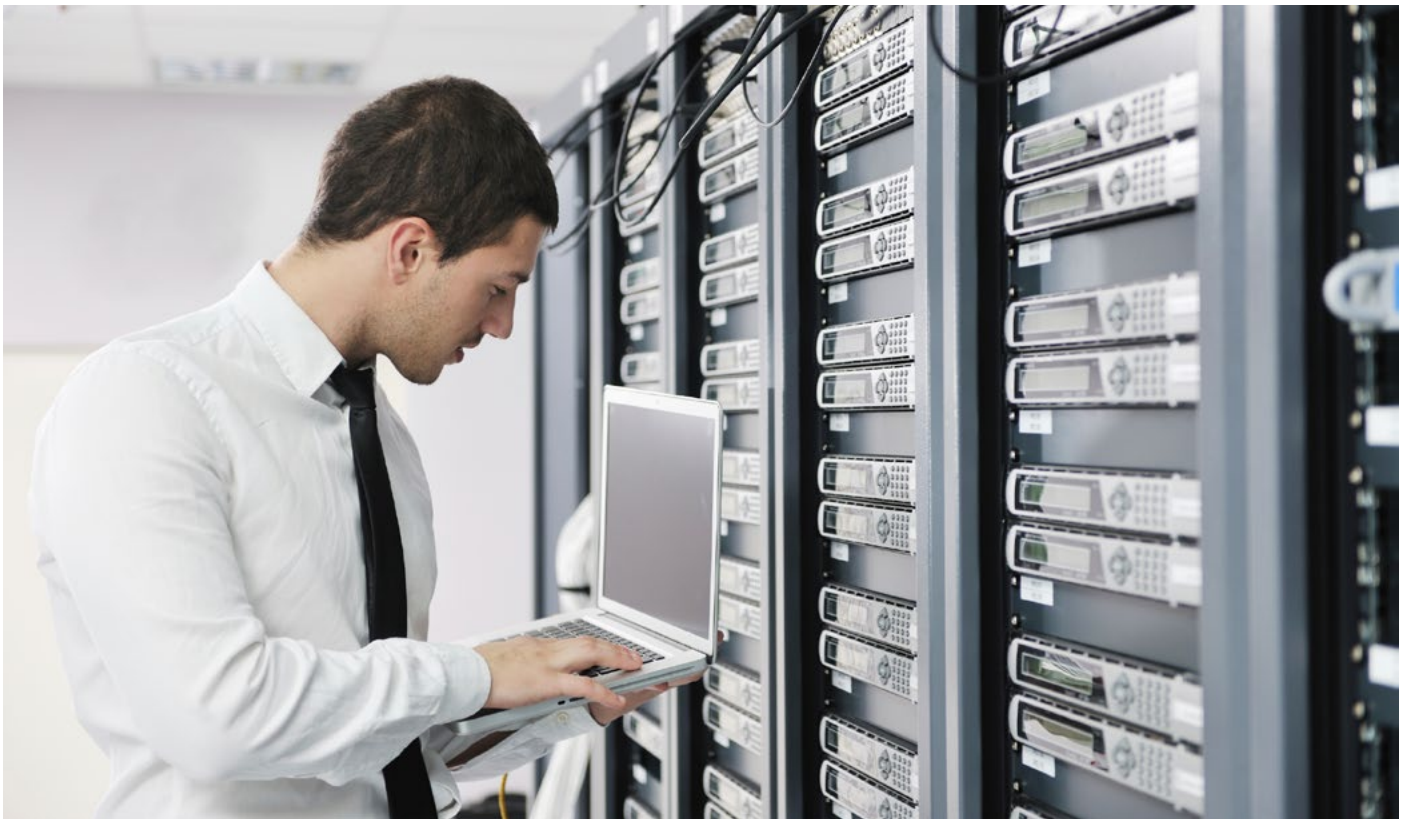
ISOTools EXCELLENCE

La norma ISO 27001

Aspectos clave de su diseño e implantación

Índice



1. El Sistema de Gestión de Seguridad de la Información (SGSI) basado en la norma ISO 27001. Aspectos claves y relación con las normas ISO 22301 e ISO/IEC 20000

Las amenazas a los activos de información

En la actualidad, las empresas se enfrentan a muchos riesgos e inseguridades procedentes de focos diversos. Esto quiere decir que los **activos de información de las empresas**, uno de sus valores más importantes, se encuentran **ligados o asociados a riesgos y amenazas que explotan una amplia tipología de vulnerabilidades.**

La seguridad de estos activos de información está en función de la **correcta gestión de una serie de factores** como: la capacidad, la elaboración de un plan de contingencia frente a los incidentes, el análisis de riesgos, las competencias, el grado de involucración de la Dirección, las inversiones en seguridad y el grado de implementación de controles.

Aunque existen muchos soportes documentales diferentes, como la información en papel o los soportes analógicos participantes, lo cierto es que, en la actualidad, la mayor parte de la información gestionada por una empresa se sustenta en la información automatizada (informatizada) a través de las nuevas herramientas de las **Tecnologías de la Información y la Comunicación (TICs).** Por este motivo, la **tendencia de la norma ISO 27001 es tratar aspectos mayoritariamente del rango informático.**

Aspectos claves de un SGSI basado en la norma ISO 27001

La norma ISO 27001 es una solución de mejora continua en base a la cual puede **desarrollarse un Sistema de Gestión de Seguridad de la Información (SGSI)** que permita **evaluar todo tipo de riesgos o amenazas** susceptibles de poner en peligro la información de una organización tanto propia como datos de terceros.

Por otro lado, también permite establecer los **controles y estrategias más adecuadas para eliminar o minimizar dichos peligros**.

Como ocurre con todas las normas ISO, la 27001 es un sistema basado en **enfoque basado en el ciclo de mejora continua o de Deming**. Dicho ciclo consiste, como ya sabemos, **en Planificar-Hacer-Verificar-Actuar**, por lo que se le conoce también como ciclo PDCA (acrónimo de sus siglas en inglés Plan-Do-Check-Act).

Trasladado a las necesidades de un SGSI, **el ciclo PDCA planteado por la ISO 27001 se dividiría en los siguientes pasos**, cada uno de ellos ligado a una serie de acciones:

PLANIFICAR	Definir la política de seguridad Establecer al alcance del SGSI Realizar el análisis de riesgo Seleccionar los controles Definir competencias Establecer un mapa de procesos Definir autoridades y responsabilidades
HACER	Implantar el plan de gestión de riesgos Implantar el SGSI Implantar los controles

CONTROLAR	Revisar internamente el SGSI Realizar auditorías internas del SGSI Poner en marcha indicadores y métricas Hacer una revisión por parte de la Dirección
ACTUAR	Adoptar acciones correctivas Adoptar acciones de mejora

Relación de la norma ISO 27001 con la ISO 22301 y la ISO /IEC 20000

La norma ISO 27001, que como hemos visto está muy enfocada en la parte informática de la empresa, se encuentra **muy ligada y tiene puntos en común con otras dos normas ISO**: la **ISO 22301** de continuidad del negocio y la **ISO/IEC 20000**, de gestión de servicios TI (Tecnología de la Información).

La **ISO 22301** trabaja el tema de la seguridad en la empresa desde una **perspectiva mucho más general y global**, tratando de asegurar la **continuidad del negocio**, lo cual influye en aspectos tan diversos como: los activos financieros, la contabilidad, los aspectos legales y todos los factores ligados con la producción y la operativa.

LAS NORMAS ISO 27001, ISO 22301 Y ISO/IEC 20000 MANTIENEN UNA RELACIÓN DE CONFLUENCIA EN CIERTOS PUNTOS PERO, SOBRE TODO, DE COMPLEMENTARIEDAD, LOGRANDO EN CONJUNTO ALTOS NIVELES DE GARANTÍA EN LO QUE RESPECTA A LA CORRECTA EVALUACIÓN, PREVENCIÓN, TRATAMIENTO Y SOLUCIÓN DE RIESGOS PARA LA EMPRESA RELACIONADOS CON LA TI.

El estándar 22301 se centra en diversos aspectos de la organización que van a **permitir su sustentabilidad**, utilizando para ello ciertos elementos y controles que van a evitar las consecuencias de las distintas amenazas, así como también encontrar las causas que motivan el problema.

Un aspecto muy importante de la norma ISO 22301, que no tiene en cuenta la 27001, son los **tiempos de recuperación**, una cuestión crucial para poder evaluar si nuestro plan de contingencia es el adecuado para poder reanudar la actividad en unos niveles aceptables para la organización, una vez ha ocurrido el incidente.

Otra noma relacionada con la ISO 27001 es el **estándar ISO/IEC 20000, de gestión de la calidad de los servicios TI (Tecnologías de la Información):** hosting, páginas web, elearning, desarrollo de software. Todo ello val ligado a la continuidad del negocio y de los servicios de información y, en conjunto, sirve para garantizar un servicio seguro, sin interrupciones importantes y de calidad.

Fases de un SGSI basado en la norma ISO 27001

En base a este sistema PDCA, la norma ISO 27001 establece las siguientes fases para elaborar un SGSI

1. Análisis y evaluación de riesgos.
2. Implementación de controles
3. Definición de un plan de tratamiento de los riesgos o esquema de mejora
4. Alcance de la gestión
5. Contexto de organización
6. Partes interesadas
7. Fijación y medición de objetivos
8. Proceso documental
9. Auditorías internas y externas

EL PROPÓSITO DE UN SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN ES, POR TANTO, GARANTIZAR QUE LOS RIESGOS DE LA SEGURIDAD DE LA INFORMACIÓN SEAN CONOCIDOS, ASUMIDOS, GESTIONADOS Y MINIMIZADOS POR LA ORGANIZACIÓN DE UNA FORMA DOCUMENTADA, SISTEMÁTICA Y ESTRUCTURADA

A continuación, **pasamos a desarrollar cada una de estas fases**.

2. Análisis y evaluación de riesgos: identificación de amenazas, consecuencias y criticidad

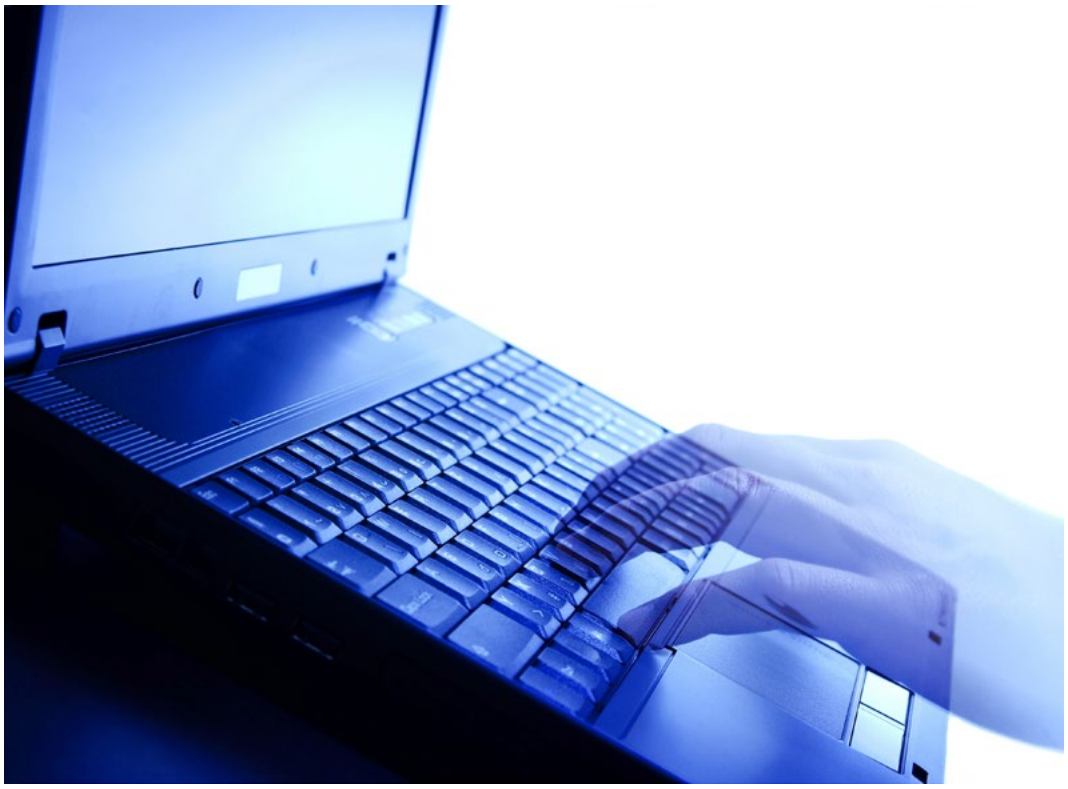
Identificación de las amenazas

Un SGSI basado en la norma ISO 27001 se fundamenta principalmente en la **identificación y análisis de las principales amenazas** para, a partir de este punto de partida, poder establecer una evaluación y planificación de dichos riesgos.

Una amenaza se puede definir como cualquier **evento que puede afectar los activos de información** y se relaciona, principalmente, con recursos humanos, eventos naturales o fallas técnicas. Algunos ejemplos pueden ser: ataques informáticos externos, infecciones con malware, una inundación, un incendio o cortes de fluido eléctrico.

Pero en ocasiones basta una omisión o despiste por parte del personal de la empresa, como el uso de una simple pulsera imantada, para que se pueda llegar a producir un daño grave, e incluso irreparable, de la información.

En definitiva, se trata de elaborar una **adecuada gestión de riesgos** que permita a las organizaciones conocer cuáles son las principales vulnerabilidades de sus activos de información.



PARA GARANTIZAR LA CORRECTA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN SE DEBEN IDENTIFICAR INICIALMENTE SUS ASPECTOS MÁS RELEVANTES.

Un correcto **proceso de identificación de riesgos** implica:

- Identificar todos aquellos activos de información que tienen algún valor para la organización.
- Asociar las amenazas relevantes con los activos identificados.
- Determinar las vulnerabilidades que puedan ser aprovechadas por dichas amenazas.
- Identificar el impacto que podría suponer una pérdida de confidencialidad, integridad y disponibilidad para cada activo.

Análisis y evaluación de los riesgos y sus consecuencias

Se debe analizar **el impacto en el negocio de un fallo de seguridad** que suponga la pérdida de confidencialidad, integridad o disponibilidad de un activo de información, **evaluando de forma realista la probabilidad de ocurrencia** de un fallo de seguridad en relación a las amenazas, vulnerabilidades e impactos en los activos.

Además de riesgo en sí, es necesario **analizar también sus consecuencias potenciales**, que son muchas y de distinta gravedad: desde una simple dispersión de la información a la pérdida o robo de datos relevantes o confidenciales.

Una **posible metodología de evaluación de riesgos** estaría compuesta de las siguientes fases:

1. Recogida y preparación de la información.
2. Identificación, clasificación y valoración los grupos de activos.
3. Identificación y clasificación de las amenazas.
4. Identificación y estimación de las vulnerabilidades.
5. Identificación y valoración de impactos: identificar, tipificar y valorar los impactos.
6. Evaluación y análisis del riesgo.

Criticidad del riesgo

Por este motivo, se deben evaluar las consecuencias potenciales para poder **evaluar su criticidad**: riesgo aceptable y riesgo residual.

Riesgo aceptable

No se trata de eliminar totalmente el riesgo, ya que muchas veces no es posible ni tampoco resultaría rentable, sino de **reducir su posibilidad de ocurrencia y minimizar las consecuencias** a unos niveles que la organización pueda asumir, sin que suponga un perjuicio demasiado grave a todos los niveles: económico, logístico, de imagen, de credibilidad, etc.

Riesgo residual

Se trata del **riesgo que permanece y subsiste después de haber implementado los debidos controles**, es decir, una vez que la organización haya desarrollado completamente un SGSI. Es un reflejo de las posibilidades de que ocurra un incidente, pese a verse implantado con eficacia las medidas evaluadoras y correctoras para mitigar el riesgo inherente.

EL RIESGO RESIDUAL PUEDE ENTENDERSE COMO LO QUE SEPARA A LAS ORGANIZACIONES DE LA SEGURIDAD ABSOLUTA

El compromiso del liderazgo

La norma ISO 27001 otorga un **peso cualitativo muy importante a la Dirección**, la cual debe ejercer el liderazgo del sistema de seguridad. A partir de aquí, se debe establecer un plan de trabajo en el que quede perfectamente definida la **segregación de tareas.** Dicho de otro modo: se tiene que establecer con exactitud quién tiene que hacer cada función y cómo ejecutarla.

Los dueños del riesgo

La norma ISO 27001 establece la **figura de Dueño del Riesgo**, asociándose cada amenaza potencial o real a un responsable, que es la persona que se asegura que se lleven a cabo las distintas actividades.

Dicho responsable no tiene por qué ser la persona que finalmente ejecuta los controles, sino alguien que se responsabiliza de que realmente los controles se están llevando a cabo acorde a lo establecido.

Por lo tanto, **es necesario definir la estructura organizacional del SGSI, seleccionado el personal idóneo** dependiendo del tamaño de la empresa y el alcance definido para la implantación del SGSI. De acuerdo a las dos anteriores variables, se puede determinar el número de profesionales con los perfiles necesarios que formarán parte del grupo de seguridad de la información de la institución.

3. La implementación de controles

Con el objetivo de que cada riesgo identificado previamente quede cubierto y pueda ser auditable, **la norma ISO 27001 establece en su última versión: ISO/IEC 27001:2013 hasta 113 puntos de control** (en la versión anterior del 2005 eran 133).

Los 113 controles están divididos por grandes objetivos:

- Políticas de seguridad de la información.
- Controles operacionales.

Cada empresa, según su parecer, puede añadir más puntos de control si lo considera conveniente, así como personalizarlos **para adaptarlos a su propio Plan de Control Operacional**, pero siempre deben estar alineados a lo que pide la norma.

4. Definición de un plan de tratamiento de los riesgos o esquema de mejora

Una vez realizado el análisis, se debe definir un **plan de tratamiento o esquema de mejora,** en el que se tengan en cuenta las **distintas consecuencias potenciales de esos riesgos**, estableciendo una criticidad para cada uno de ellos y así **poder evaluar con objetividad las diferentes amenazas.**

Formas de afrontar el riesgo

Una empresa puede **afrontar el riesgo** básicamente de **tres formas diferentes**: eliminarlo, mitigarlo o trasladarlo.

Eliminar el riego

Si el riesgo es muy crítico, hasta el punto de que pueda poner en peligro la propia continuidad de la organización, ésta debe poner todos los medios para tratar de eliminarlo, de manera que haya un **posibilidad cero de que la amenaza se llegue realmente a producir.**

Mitigarlo

En la gran mayoría de ocasiones **no es posible llegar a la eliminación total del riesgo,** ya sea porque es imposible técnicamente o bien porque **la empresa decida que no es un riesgo suficientemente crítico.** En estos casos la organización puede aceptar el riego, ser consciente de que la amenaza para la información existe y dedicarse a monitorearlo con el fin de controlarlo.

En definitiva, se trata de **implantar las medidas preventivas o correctivas necesarias** con el fin de **reducir la posibilidad de ocurrencia** o el impacto de riesgo.

Trasladarlo

Esta opción está relacionada con la **contratación de algún tipo de seguro** que compense las consecuencias económicas de una pérdida o deterioro de la información.

Sea cual el plan de tratamiento elegido por la empresa, la gestión de riesgos debe garantizar a la organización la tranquilidad de tener suficientemente identificados los riesgos y los controles pertinentes, lo cual le va a permitir actuar con eficacia ante una eventual materialización de los mismos.

En cualquier caso, a la hora de elegir una u otra opción la empresa debe **mantener el equilibrio** entre el costo que tiene una actividad de control, la importancia del activo de la información para los procesos de la empresa y el nivel de criticidad del riesgo.

Establecimiento de un rango para cada control

A cada punto de control se le debe **asociar un rango o factor determinado**. Por ejemplo, el acceso a un área segura podría dividirse en:

Rango 1. No hay establecida ninguna medida de seguridad.

Rango 2. Existe alguna medida de seguridad pero no se ha establecido una pauta concreta ni periodicidad.

Rango 3. Existen una serie de medidas establecidas, pero no se ha determinado una evaluación de las mismas.

Rango 4. Los controles tienen establecidos una periodicidad, evaluación y seguimiento.

Rango 5. Son actividades ligadas al propio negocio, es decir, se trata de un factor interno de la empresa que lo gestiona y está implementada dentro de la propia organización.

La empresa debe decidir qué tipo de rango necesita para cada control con el fin de asegurar la seguridad de la información, teniendo en cuenta que **los controles de carácter preventivo son más eficaces que los correctivos.**

Por ejemplo, es más seguro instalar un dispositivo que controle la temperatura (saltará la alarma antes de que se produzca un posible incendio) que tener un sistema anti incendio que avisa cuando ya hay humo (la situación peligrosa ya ha empezado a producirse).

Todos estos controles **siguen un ciclo de mejora continua** vinculado al plan de tratamiento de riesgos y asociados a la evaluación de los mismos para el **cálculo del riesgo residual**, que es el riesgo bruto mitigado por los controles.

Mediante el proceso de mejora continua es posible comprobar la eficacia de los controles o si es necesario cambiar de rango o factor de seguridad, realizando las modificaciones que sean necesarias.

Los controles están **incluidos en el anexo A de la norma ISO 27001** y su nivel de detalle y especificidad los diferencian de los existentes en otras normas, que tienen un carácter más generalista y transversal.

EL CONCEPTO DE CONTROL EN ESTA NORMA SE DEBE CONSIDERAR COMO UN CONJUNTO DE MEDIDAS, ACCIONES Y/O DOCUMENTOS QUE PERMITEN CUBRIR O AUDITAR CIERTOS RIESGOS

5. El alcance de la gestión

En la planeación para la implementación de un SGSI **es muy importante definir el alcance** para la implementación del sistema en una organización.

Teniendo en cuenta que existen organizaciones que difieren en tamaño por el número de empleados, volumen de información manejada, número de clientes, volúmenes de activos físicos y lógicos, número de sedes u oficinas, entre otros elementos, **se hace necesario determinar cómo se debe implantar un SGSI**.

Por ejemplo, se debe elegir en qué áreas o dependencias de la organización se desea implantar el SGSI como primera medida, cuáles posteriormente y, en algunos casos, determinar si existen ámbitos del negocio que, por sus características, no precisan de la implantación de un protocolo de seguridad.

NORMALMENTE LA DETERMINACIÓN DEL ALCANCE DE LA GESTIÓN SE REALIZA BIEN POR LÍNEAS DE NEGOCIO O POR MACRO PROCESOS. POR EJEMPLO, SI UNA EMPRESA TIENE DOS LÍNEAS DE NEGOCIO: UNA DE ASESORAMIENTO CONTABLE Y OTRO FISCAL, ES POSIBLE QUE DECIDA PRIORIZAR LA PRIMERA ACTIVIDAD, LA CONTABILIDAD, POR CONSIDERARLA MÁS VULNERABLE EN MATERIA DE SEGURIDAD DE LA INFORMACIÓN.

Por lo general, las **primeras áreas que se deben considerar** son aquellas que, por sus funciones y responsabilidades, ayudan en primera instancia a **dar cumplimiento a la misión institucional**.

Pongamos un ejemplo concreto, la determinación de alcance y priorización de una empresa comercial de tamaño mediano de compra y venta de artículos deportivos, que vende por Internet y de forma presencial en sus diferentes sedes locales y nacionales, podría ser la siguiente:

- Determinar que en primera instancia se deben cubrir áreas de contabilidad, inventario y facturación por ser un tema sensible, donde se manejan datos claves para la empresa.
- En segundo lugar, se deberían considerar la logística y atención al cliente, ya estas áreas que permiten un trato directo con los mismos pudiendo mejorar su satisfacción.
- El resto de áreas de la empresa, como el marketing, pueden no incluirse en primera instancia en el SGSI, para irse introduciendo luego de manera progresiva.

6. Contexto de organización

El **análisis de contexto de la organización** es fundamental **para el SGSI, ya que nos permite** determinar los problemas internos y externos de la organización, así como sus debilidades, amenazas, fortalezas y oportunidades que nos puedan afectar.

La norma ISO no especifica el método a utilizar para el análisis del contexto, siendo del método DAFO uno de los más comunes y aceptados. Sea cual sea el sistema elegido, es fundamental someter a valoración tanto el contexto interno (productos y servicios) como externos (logística o clima organizacional).

LA ORGANIZACIÓN DEBE PREOCUPARSE, Y POR TANTO DETERMINAR, QUÉ CUESTIONES O ASPECTOS INTERNOS Y EXTERNOS ESTÁN INVOLUCRADOS EN EL PROPÓSITO DE LA MISMA Y PUEDEN AFECTAR A LA CAPACIDAD DE ALCANZAR LOS RESULTADOS PREVISTOS PARA SU SGSI

7. Partes interesadas

Para poder realizar un correcto análisis de riesgo es preciso **definir un contexto de la organización** y comprender las necesidades y expectativas de todas las partes interesadas:

- Proveedores de servicios de información y de equipamientos de Tecnologías de la Información (TICs).
- Clientes, poniendo especial cuidado en la gestión de datos de protección personal.
- Fuerzas de seguridad de cada estado y autoridades jurídicas para tratar los aspectos legales.
- Participación en foros profesionales.
- La sociedad en general.

8. Fijación y medición de objetivos

Fijación de objetivos

Es necesario fijar unos objetivos **para la gestión de riegos**, los cuales **deben poder ser medibles,** aunque no es necesario que sean cuantificables.

Otro aspecto básico es que estos objetivos **deben ser eficientemente comunicados al conjunto de los empleados de la empresa,** puesto que todos los profesionales deben ser conscientes de que participan en un objetivo común, y que un descuido o una mala actitud pueden acarrear consecuencias muy negativas.

Además, todas las personas que trabajan en la organización deben **poseer las competencias necesarias en materia de seguridad de la información** según su puesto o función en la empresa.

Por otro lado, **cada objetivo** definido tiene que estar **asociado a unos indicadores** que permitan realizar un seguimiento del cumplimiento de las actividades.

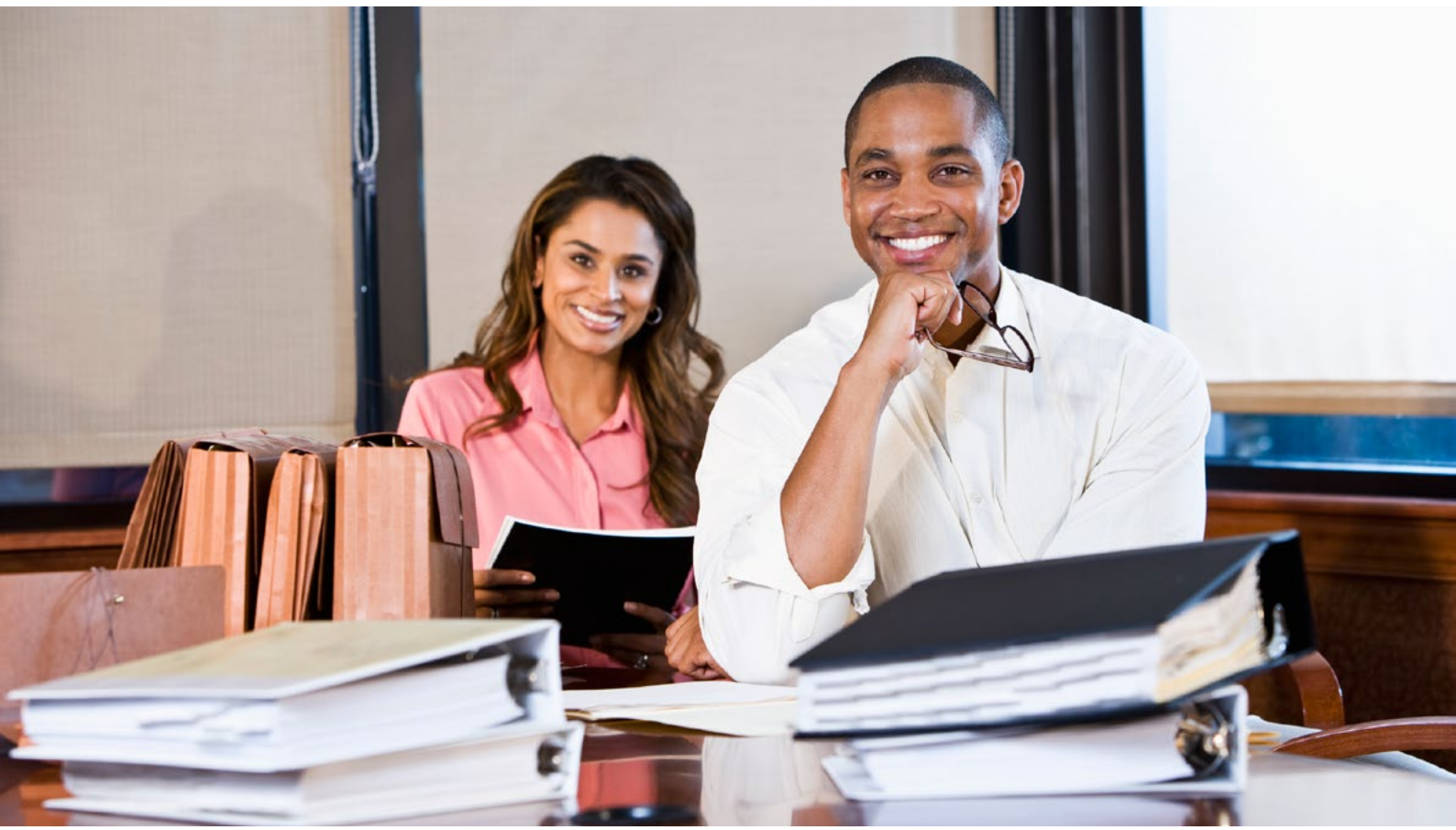
9. El proceso documental

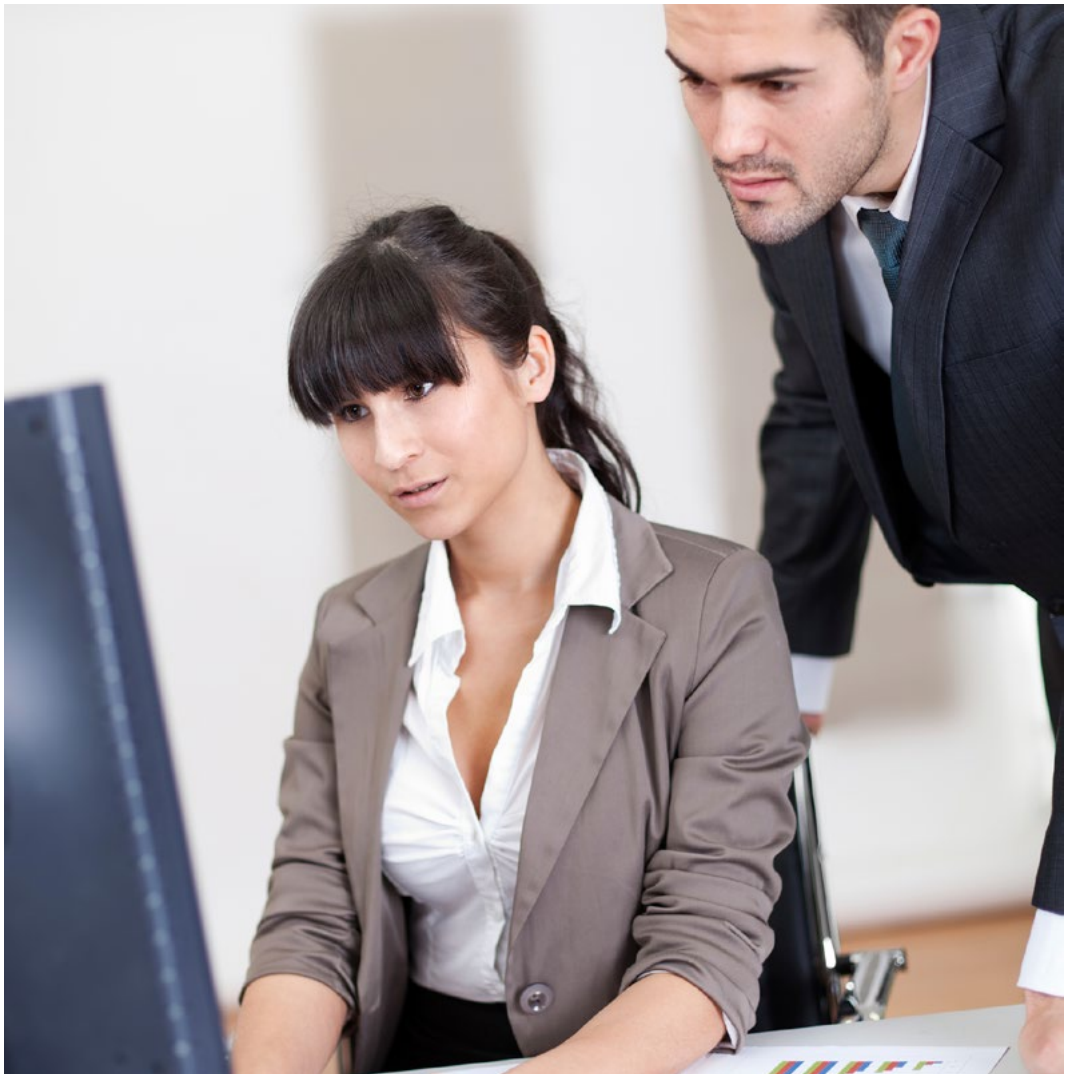
La norma ISO 27001 da mucha importancia a la **documentación**, estableciendo de manera muy estricta cómo se debe gestionar la documentación y exigiendo que la organización cuente con un procedimiento documentado para gestionar toda la información. Esta cuestión es **fundamental para la obtención de la certificación**.

La documentación puede ser presentada en diversos formatos: documentos en papel, archivos de texto, hojas de cálculo, archivos de vídeo o audio, etc. Pero en cualquier caso constituye un marco de referencia fundamental y debe estar lista en todo momento para que pueda ser consultada.

La organización debe **gestionar tanto los documentos internos** (políticas diversas, procedimientos, documentación del proyecto, etc.), **como lo externos** (diferentes tipos de correspondencia, documentación recibida con equipamiento, etc.). Por este motivo, la gestión de documentación es una tarea compleja e integral.

Con el objetivo de que las empresas gestionen eficazmente los documentos, la norma ISO 27001 **exige la aplicación de un método sistemático** para su manejo, así como la **redacción de un procedimiento para su gestión**.





10. Auditorías internas y revisión por la Dirección

Las auditorías internas

Para garantizar el correcto funcionamiento y mantenimiento de un SGSI basado en la norma ISO 27001, se hace necesario llevar **a cabo auditorías internas cada cierto tiempo** para poder comprobar que el sistema se encuentra en un estado idóneo.

Existen **dos grandes tipos de auditorías internas:**

- **Gestión**. Donde se supervisa el liderazgo, el contexto, etc.
- **Controles**. En este caso se auditan los 113 controles, normalmente se realiza por personal más experto y puede realizarse en años distintos.

Básicamente, el principal motivo de que se realicen las auditorías internas periódicamente es poder determinar si los procedimientos del SGSI se encuentran conforme a: los requisitos de la norma, la legislación vigente en cada país o sector y los objetivos marcados por la Dirección para el propio sistema de gestión.

El plan de auditoría interna

En la **planificación de la auditoría** se debe contar con el nivel de importancia de los procesos y de las áreas que van a ser auditadas y, además, hay que tener en cuenta los resultados obtenidos de auditorías previas. También es necesario definir los criterios utilizados durante la auditoría, el alcance, la frecuencia y los métodos utilizados.

Si se detectan problemas o desviaciones entre los objetivos de seguridad planteados y los resultados obtenidos, **el equipo auditor comprueba si se están aplicando las medidas necesarias, proponiendo nuevas medidas en caso necesario.**

Revisión por la Dirección

Es fundamental **realizar revisiones periódicas del SGSI por parte de la Alta Dirección** con el objetivo de comprobar el buen funcionamiento del sistema, si se están cumpliendo los objetivos y también si se está produciendo un Retorno de la Inversión (ROI).

La **Alta Dirección** de la organización es la **máxima responsable** de que el área auditada lleve a cabo las acciones necesarias para eliminar las No Conformidades que se hayan detectado durante la auditoría interna.

Ejemplos de No Conformidades pueden ser: no tener un antivirus instalado en todos los equipos, que el equipo no se encuentre encriptado o que existan contraseñas conocidas por más de una persona, cuando deberían ser unitarias o individuales.

Durante el seguimiento de las actividades realizadas, se tiene que incluir una **verificación de las acciones que se han llevado a cabo**, además de un informe en el que se plasmen los resultados obtenidos.

11. Cómo automatizar el Sistema de Gestión de Seguridad de la Información según ISO 27001

Un software de automatización permiten poder llevar a cabo una **gestión muy eficaz y exhaustiva de cualquier tipo de riesgo:** operacionales, financieros, industriales, legales u operativos, ajustándolos completamente a las necesidades de cada una de las organizaciones y facilitando, en gran medida, la adecuación a la normativa.

Algunos **aspectos a tener en cuenta** en este tipo de herramientas que facilitan la automatización de la gestión de riesgos son:

- Poner en marcha **procesos de identificación automática** de los riesgos a los que está expuesto cada organización.
- **Alinear cada riesgo con propuestas de posibles controles** para conseguir reducir los riesgos de las compañías.
- Poner en marcha un automático del **seguimiento del tratamiento** de riesgos.
- **Realizar proyecciones y simulaciones** que permitan visualizar los resultados que se podrían obtener con la implantación de los controles definidos en el plan de tratamiento de riesgos.

La Plataforma ISOTools facilita la automatización de la ISO 27001

La ISO 27001 para los SGSI es sencilla de implantar, automatizar y mantener con la Plataforma Tecnológica ISOTools.

Con ISOTools se da cumplimiento a los requisitos basados en el ciclo PHVA (Planear – Hacer – Verificar – Actuar) para establecer, implementar, mantener y mejorar el Sistema Gestión de la Seguridad de la Información, así como se da cumplimiento de manera complementaria a las buenas prácticas o controles establecidos en ISO 27002.

ISOTools también permite aplicar los requisitos de otras normas de Seguridad de la Información como PMG SSI de los Servicios Públicos de Chile, entre otros.

Este software, permite integrar la ISO 27001 con otras normas, como ISO 9001, ISO 14001 y OHSAS 18001 de una forma sencilla gracias a su estructura modular.

12. Sectores más interesados en la implementación de este sistema

Aunque la **norma ISO 27001** es perfectamente válida como guía o base para la implementación de un SGSI en cualquier empresa u organización, con independencia de su tamaño o sector, **resulta especialmente interesante**, y casi necesaria, en los **siguientes sectores**:

- **Salud**.
- **Sector público**.
- **Sector financiero**.

Sector de la salud

La definición y puesta en marcha de un SGSI basado en la norma ISO es especialmente atractiva para las organizaciones médicas, tanto públicas como privadas, por los siguientes motivos:

- La **información** que manejan es especialmente **crítica y confidencial**.
- Los requisitos y medidas planteados por la ISO 27001 garantizan la **confidencialidad y seguridad de la información de los pacientes** y trabajadores ante cualquier amenaza.
- En todo momento **se preserva la confidencialidad, integridad y disponibilidad** de la información.
- Con la aplicación de este sistema se consiguen **ventajas adicionales** como: mejorar la calidad de los servicios, disminuir los tiempos de espera o agilizar las comunicaciones internas y externas del hospital o centro de salud.

Sector público

El sector público y la administración en general también son ámbitos muy interesados en la esta norma ISO 27001. El principal motivo es que permiten poner en marcha **sistemas y protocolos que garanticen la confidencialidad y gestión adecuada de la gran cantidad de datos** que manejan, muchos de ellos personales y con un alto nivel de criticidad.

Sector financiero

La ISO 27001 es muy necesaria para el sector financiero en general, y el de las grandes empresas en particular, con el fin de **asegurar los recursos humanos y financieros de las organizaciones.**

Algunas ventajas de la certificación ISO son:

- Lograr ventaja competitiva.
- Garantizar la gestión de la calidad.
- Controlar y reducir los riesgos operativos y comerciales.
- Cumplir con la legislación y normativa de cada país y sector.
- Poner en marcha procesos de mejora continua.


ISOTools
EXCELLENCE