Sugeris®

GUÍA INFORMATIVA

ISO 27001 Explicada para Directivos

Guía completa para directivos sobre alcance, beneficios y decisiones estratégicas.

Contenido

Qué es la ISO 27001 ..... **3**

Mitos sobre la ISO 27001 ..... **5**
- La seguridad de la información es ciberseguridad 5
- La seguridad de la información sólo es responsabilidad del departamento de sistemas 6
- Una norma ISO te hace burocrático y lento 7
- ISO 27001 es muy difícil de comprender 8

Estructura de la norma ISO 27001 ..... **9**
- PDCA en la ISO 27001 9
- Perspectivas de la ISO 27001 11
- La familia ISO 27000 y las actualizaciones 13

Cláusulas del Anexo SL **16**
- Cláusula 1: Objeto y campo de aplicación 16
- Cláusula 2: Referencias normativas 16
- Cláusula 3: Términos y definiciones 16
- Cláusula 4: Contexto de la organización 16
- Cláusula 5: Liderazgo 17
- Cláusula 6: Planificación 17
- Cláusula 7: Soporte 18
- Cláusula 8: Operación 18
- Cláusula 9: Evaluación del desempeño 18
- Cláusula 10: Mejora 19

Controles de Seguridad del Anexo A **20**

Beneficios de la implementación **22**
- Comerciales 22
- Operativos 23
- De control 24
- Conceptos útiles para comprender el tema de Control 25

Contacto **27**

Sugeris®

Introducción
Qué es la ISO 27001

En la economía actual, los activos de información más críticos para las organizaciones están en formato digital facilitando su conservación, consulta y distribución.

Pero estas ventajas vienen con un gran inconveniente: los riesgos de seguridad de la información tanto por los usos y costumbres del personal en las empresas como por las características de su infraestructura cibernética y que son habitual fuente de noticias de problemas de seguridad de la información en compañías de todo tipo y tamaño.

Debido a que estos activos son valiosos y potencialmente vulnerables, debes esforzarte por protegerlos.

Para proteger la información confidencial y sensible, y para que se vea que la protegen, cada vez más organizaciones certifican su **Sistema de Gestión de Seguridad de la Información (SGSI**) con ISO 27001, que proporciona la especificación de buenas prácticas para cualquier SGSI, incorporando en su alcance tanto la información física como la digital.

La ISO 27001 contiene y describe controles específicos para proteger tu información y los repositorios y sistemas que la resguardan y administran, así como los usos y costumbres de la empresa y la conducta de su personal ante el uso constante de información diversa.

Adoptar un **enfoque proactivo** de seguridad de la información y de seguridad cibernética permitirá a tu organización **proteger sus datos y capital intelectual.**

Con una norma como la ISO 27001 también cumplirá tu empresa con las principales leyes de protección de datos y seguridad cibernética exigidas en el mundo, incluidas la *General Data Protection Regulation* (GDPR) de la Unión Europea, la *Data Protection Act 2018* (DPA) del Reino Unido y la *Directive on Security of Network and Information Systems* (NIS Directive) de la Unión Europea y Países Bajos.

Además, las empresas que buscan contratos con gobiernos o grandes clientes corporativos encontrarán cada vez más que ISO 27001 es un requisito previo para hacer negocios. La certificación se considera una poderosa garantía de tu compromiso para cumplir con tus obligaciones de seguridad y privacidad de datos con tus clientes y socios comerciales, aunque simplemente lograr el cumplimiento ya es un muy buen comienzo.

Este documento te ayudará a comprender cómo funciona ISO 27001, destacar algunos puntos clave de la implementación y explorar los beneficios de implementar un SGSI y lograr la certificación ISO/IEC 27001:2022.

Así que primero para tener más claros los conceptos necesarios veamos qué no es ISO 27001.

Mitos sobre la ISO 27001

La seguridad de la información es ciberseguridad

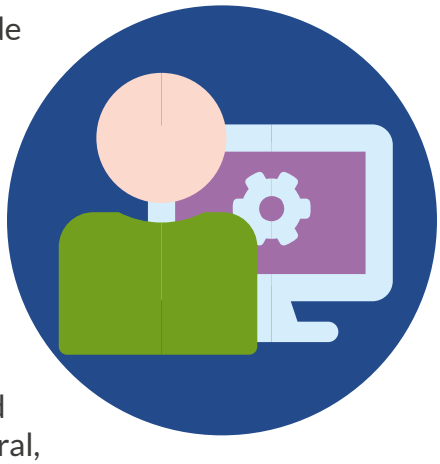
La mayoría de la gente piensa en la seguridad de la información como un problema tecnológico. Creen que cualquier cosa que tenga que ver con asegurar los datos o proteger las computadoras de las amenazas cibernéticas es algo con lo que sólo los especialistas en tecnología, y específicamente los profesionales de la seguridad informática, deben lidiar y que en una empresa no es responsabilidad del resto del personal. Esto no podría estar más lejos de la verdad.

Un **Sistema de Gestión de Seguridad de la Información (SGSI)** se refiere a toda la información circulante en la empresa y no solamente a la contenida en dispositivos de cómputo.

Por ejemplo, en una empresa de asesoría legal; la información que vale para efectos de su responsabilidad en juicios y demandas es la información original contenida en papel y la copias digitales son sólo un soporte de consulta, por lo tanto las prácticas de cómo el personal utiliza la información en papel y sus repositorios forman parte del SGSI y consecuentemente al momento de aplicar los procesos de ISO 27001 se deberán considerar aspectos como el acceso a los archiveros o muebles diversos que contienen los diferentes expedientes de los asuntos que está llevando el despacho, el control de los mismos, entradas y salidas de información a ellos, entre otros aspectos. Igual sería para una empresa de asesoría fiscal, por poner otro ejemplo.

Así que pensar que ISO 27001 es solamente ciberseguridad es un error, ES LA PROTECCIÓN DE TODA LA INFORMACIÓN SENSIBLE, que si es robada, alterada o eliminada por propios o ajenos pueda provocar algún daño a la empresa, sus clientes o sus asociados de negocio.

La seguridad de la información sólo es responsabilidad del departamento de sistemas



Como acabamos de ver la ISO 27001 certifica el Sistema de Gestión de Seguridad de la Información de la empresa, es decir DE TODA LA INFORMACIÓN SENSIBLE, y no solamente las computadoras y en general sistemas informáticos, y como la mayoría del personal requiere capturar, procesar y consultar información tanto digital como en papel, entonces es responsabilidad de todos cumplir con los requerimientos indicados por la norma para realizar estas actividades de forma segura.

Dentro de cualquier organización, las decisiones de seguridad de la información deben ser tomadas por la dirección general, no sólo por el equipo de TI; estas decisiones están, después de todo, relacionadas con los riesgos comerciales de toda la empresa e involucran a todo el personal, no solamente al que utiliza dispositivos informáticos, sino a todo aquél que debe utilizar información de la empresa para cumplir con sus responsabilidades.

ISO 27001 exige a la alta dirección la responsabilidad de definir y aprobar las políticas de seguridad de la información y además de que se asegure que quedan reflejadas en los procesos implementados y proporcionar evidencia de cuán efectivas han sido, implementando para tal objetivo el Plan Anual de Auditorías de Seguridad de la Información que la empresa debe ejecutar.

Esto último no quiere decir que las responsabilidades de seguridad de la información sólo recaen en la alta gerencia, quiere decir que además cada miembro del personal está obligado a cumplir con las políticas y procedimientos de seguridad de la información que por sus responsabilidades le apliquen.

> Es importantísimo que la empresa comprenda y haga comprender a todos los colaboradores que son una parte vital de su defensa de seguridad de la información, y que si no cumplen con el SGSI puede presentarse una vulnerabilidad significativa.

Por lo tanto, la empresa debe capacitarlos, principalmente porque los delincuentes se inclinan hacia los ataques identificados por vulnerabilidades tecnológicas o por deficiente ejecución de los procesos de seguridad de la información del negocio.

Un programa obligatorio de sensibilización del personal, junto con políticas y procedimientos documentados que establezcan las responsabilidades para proteger la información de la empresa, puede resultar invaluable cuando esta identifica que hubo un intento de robo de información infructuoso y sobre todo cuando analiza el potencial daño que pudo haber tenido si este hubiese sido exitoso.

Las políticas y procedimientos comunicados también demuestran claramente los puntos de vista de tu organización sobre la seguridad, lo que a su vez **dará a tus clientes y asociados la certeza de que su información está en manos responsables.**

Un proyecto de SGSI no necesita obligadamente ser dirigido por un experto en tecnología. De hecho, hay muchas circunstancias en las que eso podría resultar contraproducente. Los proyectos de implementación de un SGSI a menudo son dirigidos por gerentes de calidad, gerentes generales u otros ejecutivos que están en condiciones de desarrollar algo que tenga influencia e importancia en toda la organización.

Una norma ISO te hace burocrático y lento

ISO 27001 ofrece un conjunto de especificaciones, códigos de conducta y directrices sobre buenas prácticas para que las organizaciones hagan un uso seguro de sus recursos de información.

Es una norma de gestión de la seguridad de la información neutra desde el punto de vista tecnológico y del tipo de negocio de la empresa, que ofrece lineamientos para una gestión segura de la información y que además provee las especificaciones para que el SGSI sea eficaz sin provocar redundancias, burocracias o cualquier otro tipo de problema que afecte la eficiencia de la empresa.

ISO 27001, como norma universal que es, indica **qué** se debe hacer en diversos aspectos de uso de la información, pero nunca **cómo** hacerlo.

El **cómo aplicar los lineamientos** es responsabilidad de la empresa de acuerdo con sus criterios y modelo de negocio, por lo tanto, no implica que la norma sea fuente de burocracia porque la empresa se deba adaptar a esta, es lo contrario, la norma se debe implementar de acuerdo con las características de la empresa.

Este mito está muy extendido debido a que muchas empresas deciden iniciar

por su propia cuenta el estudio de la norma y no han podido asignar el personal adecuado para ello resultando en interpretaciones rigoristas de los requisitos de la norma que invariablemente terminan en *procesoesclerosis*.

Por eso una práctica muy extendida es que, si la empresa desea certificarse en el menor tiempo posible y con el menor esfuerzo y costo posible lo mejor es utilizar los servicios de una consultora especializada tanto en la norma como en el método de implementación, asegurando así una certificación exitosa.

ISO 27001 es muy difícil de comprender

La norma está redactada en un lenguaje exclusivamente empresarial, sin utilizar términos técnicos especializados o un estilo de redacción rebuscado. Por el contrario: está redactada en un lenguaje claro y directo, sin ambigüedades ni posibilidad de que los requerimientos puedan ser interpretados de diversos modos o en formas contradictorias.

Como está diseñada para cualquier tipo de empresa en la que la información es un activo muy importante y que requiere un manejo seguro, está en un lenguaje en que sea comprendido por todo tipo de organizaciones.

Posiblemente este mito se ha extendido porque las empresas caen en el error de designar la tarea de interpretar la norma a personal de bajo nivel organizacional, quizá hasta operativo, que generalmente no entiende el lenguaje gerencial o de negocios que utiliza la norma.

> La protección de la información no es un fin en sí mismo para la norma, su objetivo es que los procesos de la empresa y la consecución de sus objetivos de negocio no se vean afectados debido a robo, alteración o destrucción de su información.

Al no ser una norma técnica, cuando se encarga un proyecto de certificación ISO 27001 exclusivamente a personal técnico de TI este no alcanza a comprender completamente los requerimientos de la norma y termina haciendo difícil, engorrosa y burocrática su implementación, al adoptar un punto de vista rigorista motivado por el temor de no lograr la certificación.

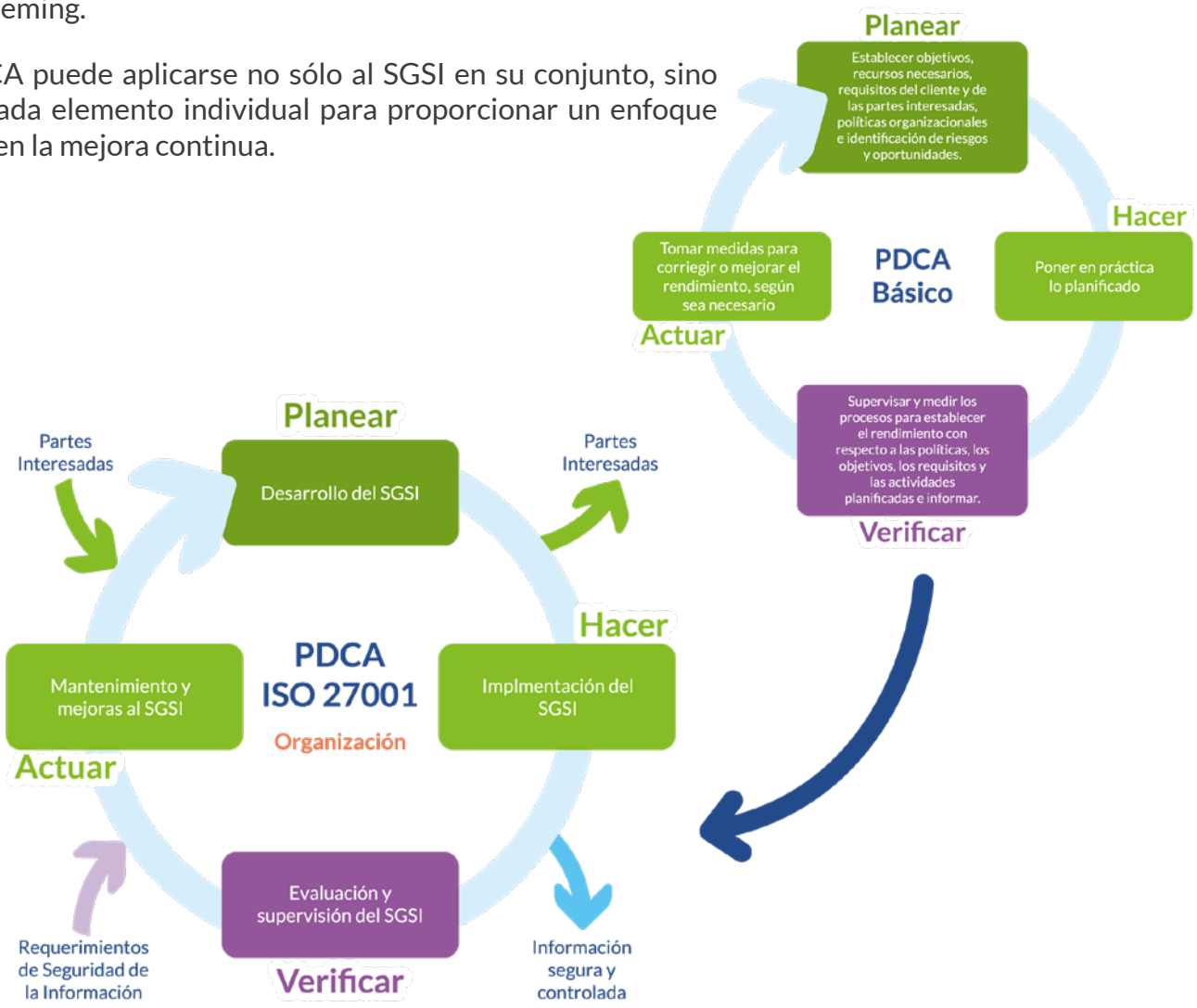
Así que, lo más recomendable es que se forme un grupo multidisciplinario para su implementación en el que estén incluidos los niveles gerenciales, ya que su perspectiva pondrá la implementación en un marco eficaz pero pragmático, logrando así que la norma aporte valor a la empresa y no solamente seguridad.

Estructura de la norma ISO 27001

PDCA en la ISO 27001

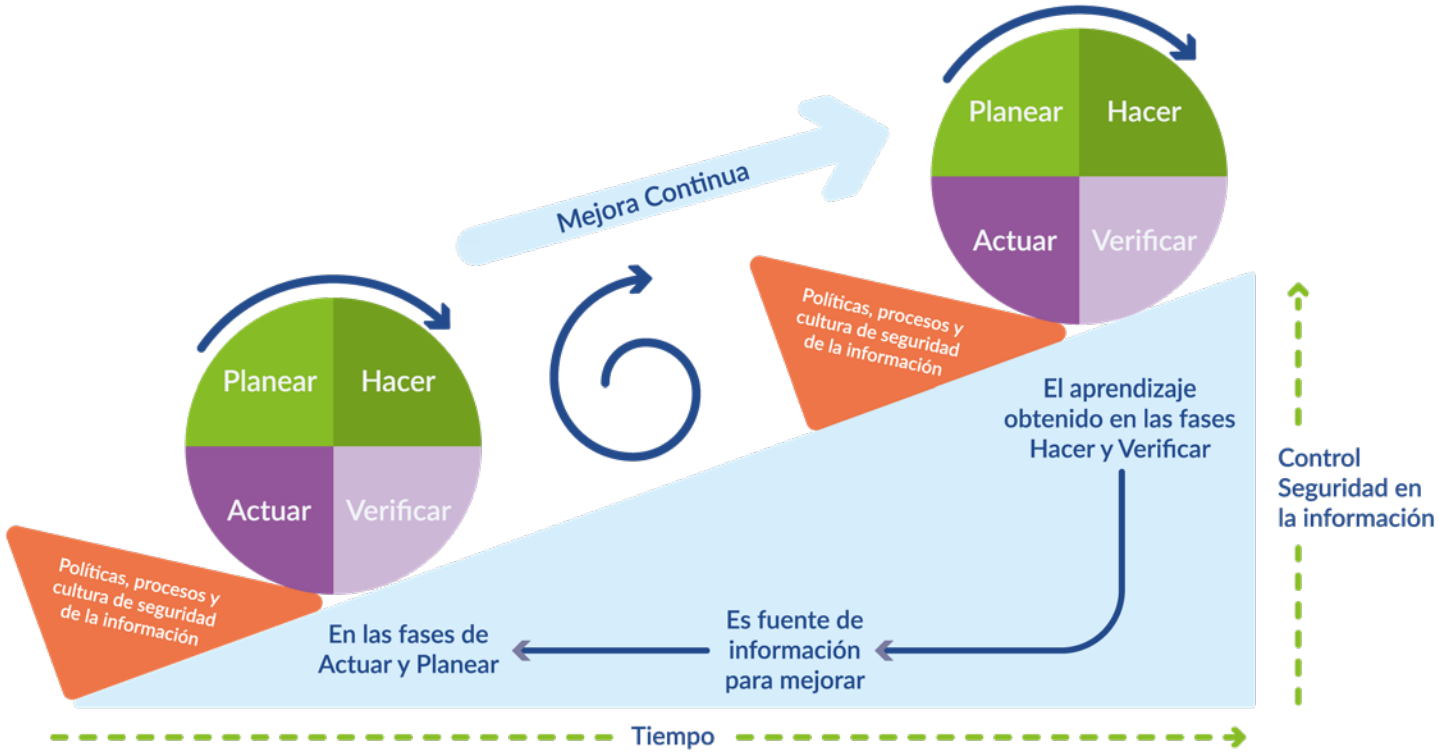
La norma ISO 27001 se basa en el ciclo Planificar-Hacer-Verificar-Actuar (PDCA por sus siglas en inglés), también conocido como Círculo de Deming.

El ciclo PDCA puede aplicarse no sólo al SGSI en su conjunto, sino también a cada elemento individual para proporcionar un enfoque persistente en la mejora continua.



Como el círculo de Deming es un sistema de bucle cerrado se garantiza que el aprendizaje obtenido en las fases **Hacer y Verificar** se utilice para informar las fases **Actuar y Planear** posteriores, logrando una mejora continua.

Aunque parece un sistema cíclico, es una **espiral ascendente**, ya que el aprendizaje hace avanzar a la empresa cada vez que se cumple el ciclo, como se muestra en la gráfica siguiente:



Perspectivas de la ISO 27001

Para hacerla comprensible, la norma utiliza tres perspectivas o puntos de vista generales para abordar el diseño de un SGSI eficaz y son las siguientes:

1. Perspectiva de Gobernanza
Los objetivos de seguridad de la información y de seguridad de TI deben ser derivados de los objetivos generales de la empresa y no al revés.

2. Perspectiva de Riesgo

a. Requisitos de protección y exposición al riesgo de activos informativos y sistemas informáticos de la empresa para cumplir con sus objetivos de negocio y conservación del valor de marca de esta.
b. Actitud de la empresa ante el riesgo.
c. Oportunidades frente a riesgos.

3. Perspectiva de Cumplimiento

a. Reglamentos externos establecidos por leyes, reguladores y normas.
b. Reglamentos y directrices internos.
c. Obligaciones contractuales.

Estas perspectivas determinan:

→ Qué medidas de protección son las más adecuadas y eficaces para las oportunidades y los procesos de la empresa.

→ El nivel de protección requerido con respecto a la criticidad de los activos de la empresa en cuestión de cumplimiento de las leyes y reglamentos aplicables.


Administración de la empresa
Indicadores clave, capacitación y entrenamiento al personal, informes de incidentes de seguridad, informes de auditorías internas de cumplimiento, vigencia de la matriz de riesgos, vigencia y actualización del Sistema de Gestión de Seguridad de la Información.
Objetivos de la empresa
Riesgos de la empresa
Objetivos legales y contractuales de la empresa
Gobernanza
Implementación y cumplimiento de acuerdo con los objetivos de la empresa
Administración de riesgos
Identificación, evaluación y administración de riesgos.
Cumplimiento
Implementación y cumplimiento con los requisitos de la norma, contratos y disposiciones legales.
Cumplimiento
Vulnerabilidades
Políticas
Sistema de Gestión de Seguridad de la Información
Cumplimiento y vigencia
Requerimientos y controles
Políticas, procesos, procedimientos, prácticas, cultura organizacional, indicadores.
Evaluación de vulnerabilidades
Auditorías internas de cumplimiento, incidentes de seguridad, actualización de la matriz de riesgos.
Objetivos empresariales
Alineamiento de los requerimientos de seguridad para participar en el cumplimiento de los objetivos de la empresa.

La familia ISO 27000 y las actualizaciones

La serie de normas 27000 nació en 1995 como BS7799 y fue redactada por el Departamento de Comercio e Industria (DTI) del Reino Unido. Las normas se denominan realmente como "ISO/IEC" porque son desarrolladas y mantenidas conjuntamente por dos organismos internacionales de normalización: ISO (*International Organization for Standardization*, www.iso.org) y la IEC (*International Electrotechnical Commission*, www.iec.ch). Sin embargo, para simplificar, en el uso cotidiano se suele omitir la parte "IEC".

Actualmente hay 45 normas publicadas en la serie ISO 27000. De ellas, la ISO 27001 es la única norma destinada a la certificación del Sistema de Gestión de Seguridad de la Información. Las demás normas ofrecen orientación sobre la aplicación de las mejores prácticas. Algunas orientan sobre cómo desarrollar un SGSI para sectores concretos, otras orientan sobre cómo implementar procesos y controles clave de gestión de riesgos para la seguridad de la información, pero la 27001 es la que contiene los requisitos que se deben cumplir para obtener la certificación oficial.

Se realizan revisiones y actualizaciones periódicas cada cinco años para determinar si es necesario renovarlas.

La actualización más reciente de la norma ISO 27001 fue en el mes de octubre del 2022. La versión anterior fue publicada en el año 2013 aunque con algunos cambios en esos nueve años entre una versión y otra, esta nueva versión toma en cuenta las actuales formas de trabajar que se han presentado, sobre todo derivadas de la pandemia de COVID-19, incluyendo el trabajo remoto y la adopción cada vez más frecuente de servicios en la nube.

Más que cualquier otro fenómeno, el teletrabajo ha traído nuevos riesgos provocando que el perímetro de seguridad de las empresas se haya extendido hasta los hogares del personal que trabaja en ellas, o quizá aún más allá, llegando a comercios como cafés internet, a los que con frecuencia acuden algunas personas para realizar parte de su trabajo, por lo que los Sistemas de Gestión de Seguridad de la Información ahora deben tomar en cuenta estas fuentes de riesgos.

Debido a esta tendencia el origen de los riesgos se ha multiplicado varias veces, además de que la evolución de la tecnología digital ha incorporado una gran gama de dispositivos que no existían desde la versión 2013.

> El internet de las cosas es una tendencia aún en sus primeras etapas de desarrollo y comercialización, pero que eventualmente representará un enorme reto a todas las organizaciones, sin importar su tamaño o actividad de negocio.

Esto está provocando que constantemente se generen conceptos y herramientas que hace poco no eran importantes o trascendentales para la seguridad de la información.

La actualización intermedia más importante se realizó en 2012 cuando la ISO publicó el Anexo SL. Este cambio fue de gran mejora ya que se estructuró la norma en un esquema más sencillo de entender, aplicado a todas las normas ISO de sistema de gestión y no solamente a la 27001.

Esta modificación surge debido a que empresas de diversos tipos de actividad tenían la misma necesidad de implementar un Sistema de Gestión de Seguridad de la Información y como existía (y aún existe) el mito de que la norma es solamente sobre ciberseguridad, estas no encontraban cuál era la norma "que les aplicaba", ya que tenían información en papel, video o cualquier otro medio.

Además, algunas empresas ya contaban con otras certificaciones como ISO 9000, ISO 14000 o ISO 20000 y se confundían tomando toda la norma 27001 provocándoles burocracia y actividades redundantes, algo totalmente innecesario por el hecho de que las normas ISO que están orientadas a los sistemas de gestión tienen requisitos, términos y definiciones comunes.

Por ejemplo, en todas las normas de gestión se exigen análisis del contexto de la organización y de liderazgo, por citar dos ejemplos, entonces estos conceptos son comunes a cualquier norma y por lo tanto pueden ser tomados en cuenta si la empresa ya tiene una certificación ISO previa, ahorrándole a la organización realizar nuevamente todo el proceso y aprovechar lo ya trabajado para solamente complementarlo con las exigencias de la nueva norma que se desea implementar. Esto claramente trae eficiencias a la empresa que resultan en un plazo de implementación más corto.

Por lo tanto, la ISO mediante el Anexo SL estructuró todas las normas de sistemas de gestión en 10 apartados o cláusulas de acuerdo con la tabla siguiente, ofreciendo que todas las futuras normas de sistemas de gestión tendrán la misma estructura de referencia, texto básico idéntico, así como términos y definiciones comunes. Esto centra las características específicas de la norma en las cláusulas 6 a la 9 y por lo tanto facilita el trabajo de implementación a las empresas que ya cuentan con una norma ISO de algún sistema de gestión.

Anexo SL

Cláusula 1	Objeto y campo de aplicación
Cláusula 2	Referencias normativas
Cláusula 3	Términos y definiciones
Cláusula 4	Contexto de la organización
Cláusula 5	Liderazgo
Cláusula 6	Planificación
Cláusula 7	Soporte
Cláusula 8	Operación
Cláusula 9	Evaluación del desempeño
Cláusula 10	Mejora

Cláusulas del Anexo SL

Cláusula 1: Objeto y campo de aplicación

Trata sobre el alcance de los resultados esperados del sistema de gestión, cuando se trate de 27001 entonces serán los resultados esperados por la implementación de esta norma. Los resultados deben ser específicos de empresa y coherentes con el contexto de esta.

Cláusula 2: Referencias normativas

Contiene detalles sobre las normas de referencia o publicaciones relevantes en relación con la norma concreta, en nuestro caso ISO 27001.

Cláusula 3: Términos y definiciones

Explica términos y definiciones aplicables a la norma específica (en nuestro caso ISO 27001), además de cualquier otro término y definición relacionado con la norma.

Cláusula 4: Contexto de la organización

Determina por qué la organización está donde está, es lo que es y tiene los problemas que tiene. En esta parte de la norma la organización debe identificar las condiciones internas y externas que pueden influir en los resultados esperados al implementar la norma, así como a todas las partes interesadas y sus necesidades.

También debe documentar su alcance y establecer los límites del SGSI, siempre en línea con los objetivos de negocio.

Analiza centralmente los siguientes aspectos:

a. Conocimiento de la organización y de su contexto.
b. Comprensión de las necesidades y expectativas de las partes interesadas.
c. Determinación del alcance del sistema de gestión.
d. Sistema de gestión.

Cláusula 5: Liderazgo

A partir de esta modificación, como nunca, las normas ISO en cuanto al sistema de gestión, hacen especial insistencia en el liderazgo, no sólo en los mandos medios, que figuraban en las normas anteriores como principales impulsores del sistema de gestión, sino que ahora exige a la alta dirección una mayor responsabilidad y participación. Le responsabiliza de la integración de los requisitos del sistema de gestión en los procesos del negocio y le demanda que se asegure de que el sistema de gestión logre los resultados previstos y que asigne los recursos necesarios. Además, la alta dirección es también responsable de comunicar la importancia del sistema de gestión y aumentar la toma de conciencia y la participación del personal.

Analiza centralmente los siguientes aspectos:

a. Liderazgo y compromiso.
b. Política.
c. Roles, responsabilidades y autoridades en la organización.

Cláusula 6: Planificación

Específicamente para ISO 27001, orienta sobre la forma concreta de tratar el riesgo. Una vez que la organización ha definido sus riesgos y oportunidades tiene que establecer cómo van a ser tratados a través de la planificación.

En esta parte de la norma se impulsa un enfoque proactivo que sustituye al comportamiento reactivo reduciendo la necesidad de acciones correctivas.

Además, se exige que los objetivos del SGSI sean medibles, que se les dé seguimiento, que sean comunicados, que sean coherentes con la política del SGSI y estén permanentemente actualizados.

Analiza centralmente los siguientes aspectos:

a. Acciones para tratar riesgos y oportunidades.
b. Objetivos del sistema de gestión y planificación para lograrlos.

Cláusula 7: Soporte

Después de que la empresa ha analizado el contexto, el compromiso necesario y la planificación de su SGSI, tiene que asegurar el soporte requerido para cumplir con sus metas y objetivos. Incluye los recursos necesarios, comunicaciones internas y externas e información documentada que sirva como guía para que todo el personal de la empresa cumpla con los requerimientos del SGSI.

Analiza centralmente los siguientes aspectos:

a. Recursos.
b. Competencia.
c. Toma de conciencia.
d. Comunicación.
e. Información documentada.

Cláusula 8: Operación

En esta parte de la norma se encuentra el corazón de la misma y por lo tanto la mayor parte de los requisitos del SGSI. Esta parte establece tanto los procesos internos como los contratados externamente, incluyendo los criterios adecuados para el control de estos, así como las formas de gestionar los cambios planificados y los de urgencia.

Analiza centralmente el siguiente aspecto:

a. Planificación y control operativo.

Cláusula 9: Evaluación del desempeño

Es esta parte la norma exige que las organizaciones determinen los qué, cómo y cuándo necesarios para una supervisión adecuada de los objetivos del SGSI, así como su medición, análisis y evaluación.

Además, se hace una aportación valiosísima que por fin ha quedado como una exigencia de cumplimiento para la certificación y nos referimos a la función de auditoría interna. Un proceso integrante del sistema de gestión para asegurar que se ha implementado, mantenido y ejecutado con éxito y que la alta dirección de manera rutinaria realiza la revisión necesaria para asegurarse de que el SGSI es apropiado, adecuado y eficaz.

Analiza centralmente los siguientes aspectos:

a. Seguimiento, medición, análisis y evaluación.
b. Auditoría interna.
c. Revisión por la dirección.

Cláusula 10: Mejora

También es valiosísimo este cambio ya que se vuelve criterio de cumplimiento exigible para la certificación que la organización esté continuamente atenta a actividades de innovación, mejora y corrección para asegurarse de que su SGSI se mantiene apto para cumplir con sus objetivos.

Analiza centralmente los siguientes aspectos:

a. No conformidad y acción correctiva.
b. Mejora continua.

De esta forma, la ISO ha estructurado la nueva versión de ISO/IEC 27001:2022 y si comparas esta norma con cualquier otra de sistemas de gestión verás que su estructura es idéntica.

Así que si tu organización ya tiene un sistema de gestión certificado con alguna norma ISO o si después de certificarte en la 27001 tienes planeado certificar con ISO algún otro sistema de gestión verás que ya cumples con una parte de los requerimientos y solamente tendrás que agregar el componente particular que corresponde al sistema de gestión específico de que se trate.

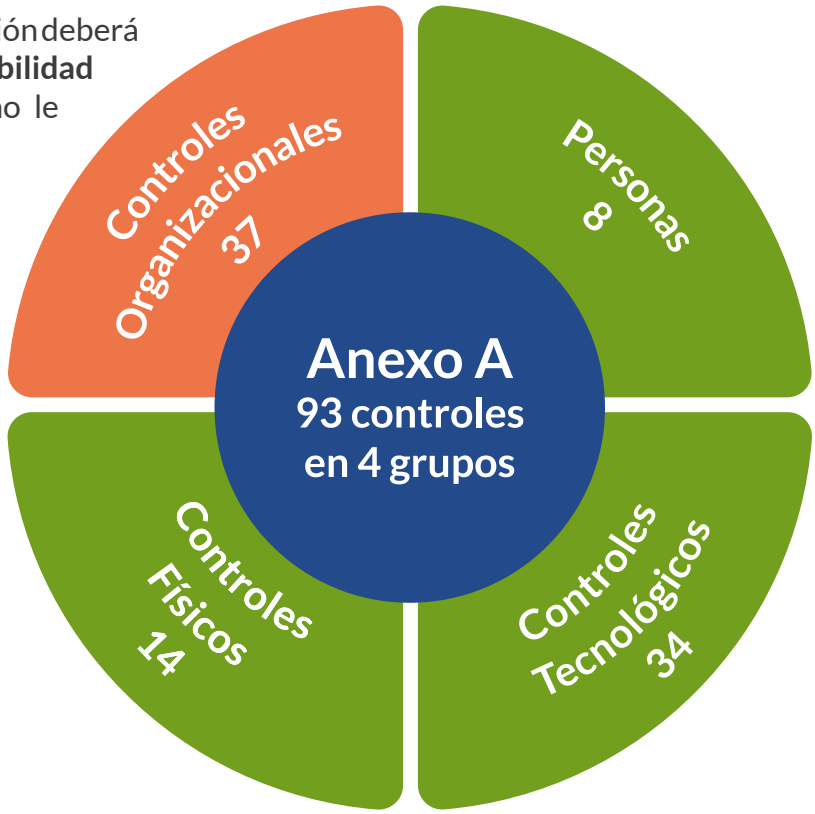
Controles de Seguridad del Anexo A

Los controles del Anexo A son las **prácticas concretas** para lograr un eficaz Sistema de Gestión de Seguridad de la Información (SGSI).

Es importante aclarar que puede darse el caso de que, para una empresa, por su particular tipo de negocio o tipo de información, no todos los controles de seguridad le sean obligatorios. No obstante, debe analizar cuáles sí son aplicables para poder certificar su sistema de gestión.

Por lo tanto, para cada control, la organización deberá establecer una **Declaración de Aplicabilidad (SOA)** justificando la razón por la que no le aplica.

La norma contiene 93 controles organizados en 4 grupos:



Cada control presenta información adicional sobre atributos o características que pueden ayudar a su categorización y monitoreo. Por ejemplo, para el control tecnológico 8.12, Prevención de Fuga de Datos, nos dice que “Las medidas de prevención de fuga de datos deben aplicarse a los sistemas, redes y cualquier otro dispositivo que procese, almacene o transmita información confidencial”. Y así para cada uno.

Además, el Anexo A caracteriza cada control con 5 atributos:

Atributos de los Controles

1. Tipo de Control

Evalúa cuándo y cómo el control modifica el riesgo con respecto a la ocurrencia de un incidente de seguridad de la información.

Los controles pueden ser:

a. Preventivos
b. Correctivos
c. Predictivos

2. Propiedades de la Seguridad de la Información

Establece cuáles de las siguientes características de la información contribuirán a definir el control:

a. Confidencialidad
b. Integridad
c. Disponibilidad

3. Conceptos de Ciberseguridad

Ofrece las siguientes actividades aplicables a los controles de seguridad:

a. Identificar
b. Proteger
c. Detectar
d. Responder
e. Recuperar

4. Capacidad operativa

Explica a qué tipo de macroproceso pertenece el control de acuerdo con su aporte de valor:

a. Gobernanza
b. Gestión de Activos
c. Protección de la Información

5. Dominios de Seguridad

Ayuda a identificar el atributo de cada control para caracterizarlo desde la perspectiva de cuatro dominios de seguridad de la información:

a. Gobernanza
b. Protección
c. Defensa
d. Resiliencia

Beneficios de la implementación

Comerciales

Contar con la aprobación de un SGSI por parte de un tercero independiente puede proporcionar a una organización una ventaja competitiva o permitirle "alcanzar" a sus competidores.

Los clientes que están expuestos a riesgos significativos con su información exigen cada vez más a sus proveedores la certificación ISO 27001.

Cuando el cliente también está certificado en ISO 27001, a mediano plazo optará por trabajar únicamente con proveedores en cuyos controles de seguridad de la información confíe y que tengan la capacidad de cumplir sus requisitos contractuales, así que para estar más seguro y no tener que hacer una inspección que le representará costo y tiempo decide exigir la certificación vigente.

Para las organizaciones que deseen trabajar con este tipo de clientes, disponer de un SGSI con certificación ISO 27001 es un requisito clave para mantener y aumentar sus ingresos comerciales.

En la actual economía basada en el conocimiento, casi todas las organizaciones dependen de la seguridad de la información clave. La implantación de un SGSI formal es un método probado para proporcionar dicha seguridad.

La norma ISO 27001 es un marco reconocido internacionalmente para un SGSI de buenas prácticas y su cumplimiento puede verificarse de forma independiente para mejorar la imagen de una organización y dar confianza a sus clientes.

Es importante que comprendas que esta tendencia sigue creciendo en el mundo a un ritmo anual del 27%, es decir que eventualmente será un requisito o *commodity* entre todos los clientes y proveedores cuyas empresas tengan más de 20 colaboradores.

La mayoría de las organizaciones reconocen ahora que no es cuestión de si se verán afectadas por una violación de la seguridad de su información, sino de cuándo.

Operativos

Como la norma ISO 27001 apoya el desarrollo de una cultura interna para que el personal esté alerta a los riesgos de seguridad de la información y desarrolle un enfoque coherente para enfrentarlos, incluyendo comportamientos y tecnología, logra que la organización diseñe controles más sólidos para enfrentar estas amenazas dándole agilidad en sus respuestas para que le permita que sus acciones sean fundamentalmente proactivas y muy poco reactivas logrando el objetivo fundamental de la norma: INFORMACIÓN BAJO CONTROL.

Un plan proactivo siempre te dará el mejor control de seguridad y optimización de costos.

También minimiza el costo de la implementación de un sistema informativo seguro ya que contiene las mejores prácticas evitándole a tu organización una ruta de prueba y error. Y si aun así se te presenta un incidente de seguridad las consecuencias se reducirán al mínimo y las mitigarás con mayor eficacia.

Si deseas iniciar por tu propia cuenta un análisis de qué tan preparada está tu empresa para abordar un proyecto de certificación en ISO 27001 te recomendamos esta herramientaque encontrarás en nuestro sitio web:

De control

Muchas organizaciones tienen información que es crítica para sus operaciones, vital para mantener su ventaja competitiva o una parte inherente de su valor financiero.

Contar con un SGSI sólido y eficaz permite a los propietarios y directivos de las empresas responsables de la gestión de riesgos estar más tranquilos sabiendo que no están expuestos al riesgo de multas cuantiosas, interrupciones importantes del negocio o un golpe significativo a su reputación.

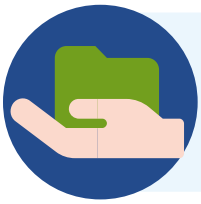
Los tipos de riesgo para la seguridad de la información se denominan comúnmente como **CIA** (*Confidentiality*, *Integrity*, *Availability*).

a. **Confidencialidad:** Cuando una o varias personas acceden sin autorización a la información.
b. **Integridad:** Cuando se modifica el contenido de la información de modo que deja de ser exacta o completa y no se conoce la persona, motivo y momento de la modificación.
c. **Disponibilidad:** Cuando se pierde el acceso a la información sin conocer las causas ni el momento en que se perdió ni cómo recuperarlo.

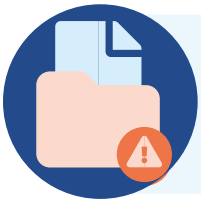
Los riesgos en la seguridad de la información suelen surgir debido a la presencia de amenazas y vulnerabilidades en los activos que procesan, almacenan, guardan, protegen o controlan el acceso a la información que da lugar a incidentes.

En este contexto, los activos suelen ser personas, equipos, sistemas o infraestructuras.

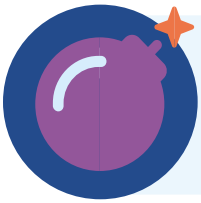
Conceptos útiles para comprender el tema de Control



La **información** es el conjunto o conjuntos de datos que una organización desea proteger, como los expedientes del personal, los expedientes de los clientes, los expedientes financieros, los datos de diseño, los datos de pruebas, etc.



Los **incidentes de seguridad** provocan una pérdida de confidencialidad (por ejemplo, una violación de datos), integridad (por ejemplo, la corrupción de datos) o disponibilidad (por ejemplo, un fallo del sistema).



Las **amenazas** provocan los incidentes y pueden ser malintencionadas (por ejemplo, un robo), accidentales (por ejemplo, un error al pulsar una tecla) o un caso fortuito (por ejemplo, una inundación).

Vulnerabilidades como ventanas abiertas en las oficinas, errores en el código fuente o la ubicación de edificios junto a ríos aumentan la probabilidad de que la presencia de una amenaza dé lugar a un incidente no deseado y costoso.

En seguridad de la información, el riesgo se gestiona mediante **el diseño, la implantación y el mantenimiento de controles** como ventanas cerradas con llave, pruebas de software o la ubicación de equipos vulnerables por encima del nivel del suelo.

Un Sistema de Seguridad de la Información o SGSI que cumple con la norma ISO 27001 tiene un conjunto interrelacionado de procesos de mejores prácticas que facilitan y apoyan el diseño, la implementación y el mantenimiento adecuados de los controles.

Los procesos que forman parte de un SGSI suelen ser una combinación de los **procesos empresariales básicos existentes** (por ejemplo, contratación, iniciación, formación, compras, diseño de productos, mantenimiento de equipos, prestación de servicios) **y los específicos para mantener y mejorar la seguridad de la información** (por ejemplo, gestión de cambios, copias de seguridad de la información, control de acceso, gestión de incidentes, clasificación de la información).

Si se hace eficazmente, hay beneficios de control significativos para aquellas organizaciones que dependen de la protección de información valiosa o sensible.

Estos beneficios pueden resumirse en lograr anular las tres características CIA de riesgos: Confidencialidad, Integridad y Disponibilidad.

¡Eso es todo!

Aunque podríamos seguir incluyendo información sobre la ISO 27001, consideramos que con lo expuesto es suficiente para que comprendas adecuadamente lo que implica esta norma y los beneficios que aportará a tu organización.

Si tienes alguna pregunta o inquietud adicional sobre ISO 27001 y los Sistemas de Gestión de Seguridad de la Información, contáctanos y con gusto responderemos a tus cuestionamientos.

Esperamos que tu empresa pronto ostente la certificación ISO/IEC 27001:2022 en su sitio web, publicidad e instalaciones, para beneficio de sus objetivos comerciales, su valor de marca y de sus clientes.

El equipo de consultoría de Sugeris