Sistema de gestión de la seguridad de la información, importancia en las empresas

L.C.P. Martín Ernesto Quintero Garcia

Introducción

La información es fundamental para toda empresa y requiere que se proteja ante cualquier amenaza que la pueda poner en peligro las empresas tanto públicas como privadas, pues podría dañarse la salud empresarial. La realidad nos muestra que las empresas enfrentan en la actualidad con un alto número de riesgos e inseguridades procedentes de una amplia variedad de fuentes, entre las que se encuentran los nuevos negocios y nuevas herramientas de las tecnologías de la información y la comunicación (TIC), que los CEO (directores generales) y CIO (directores de informática) deberían aplicar. Todas estas herramientas deben aplicarse según los objetivos empresariales con la mayor seguridad, y garantizar la confidencialidad (asegurando que sólo quienes estén autorizados pueden acceder a la información), integridad (garantizando que la información fiable y exacta) y disponibilidad (asegurando que los usuarios autorizados tienen el acceso debido a la información).

La información, como uno de los principales activos de las organizaciones, debe protegerse a través de la implantación, mantenimiento y mejora de las medidas de seguridad para que cualquier empresa logre sus objetivos de negocio, garantice el cumplimiento legal, de prestigio y de imagen. Al respecto, el ***Sistema de gestión de la seguridad de la información (SESI) ISO27001,*** es la solución de mejora continua más adecuada para evaluar los riesgos físicos (incendios, inundaciones, sabotajes, vandalismos, accesos indebidos e indeseados) y lógicos (virus informáticos, ataques de intrusión o denegación de servicios) y establecer las estrategias y controles adecuados que aseguren una permanente protección y salvaguarda de la información.

Aspectos básicos de la ISO 27001

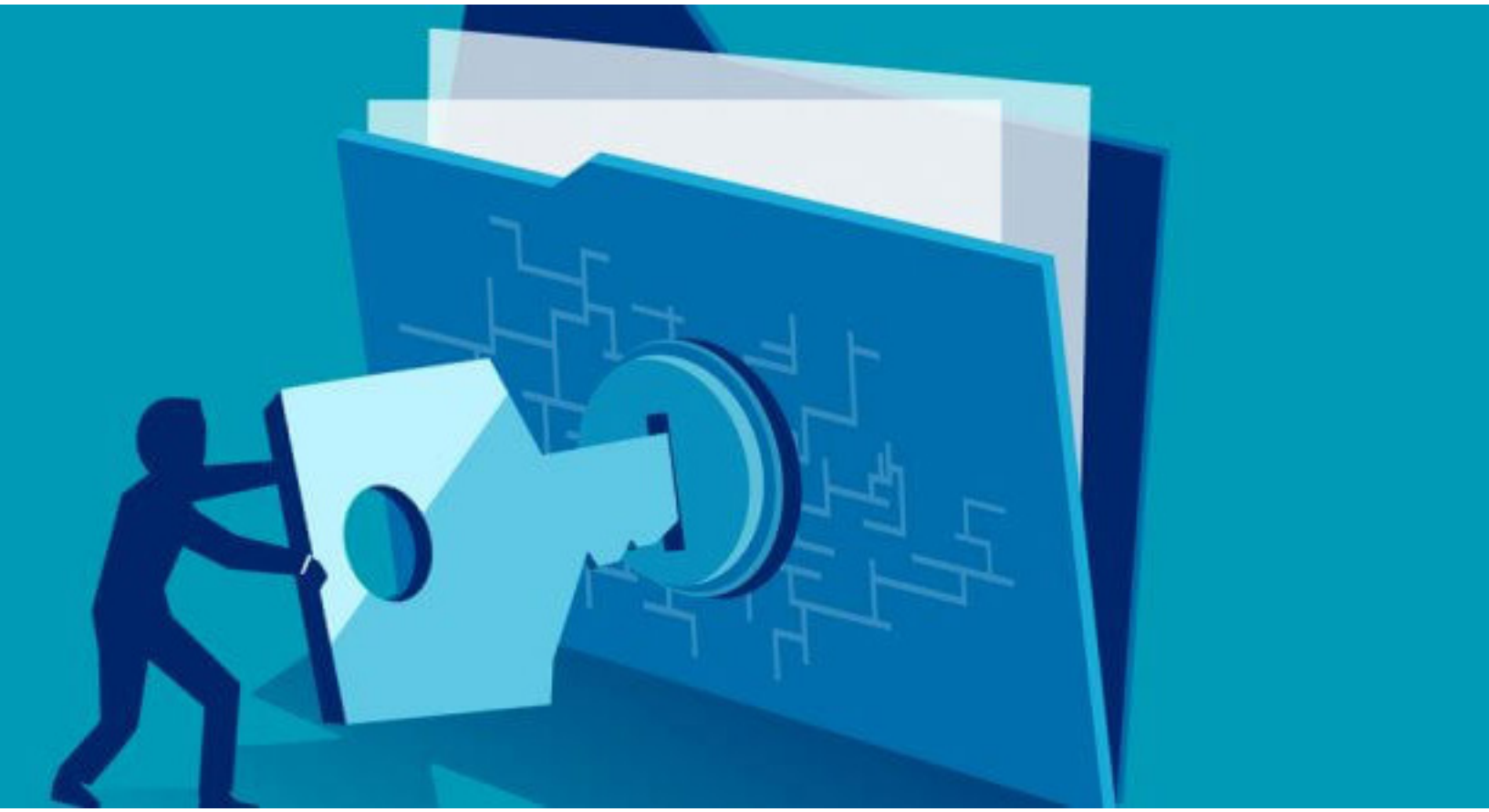
Es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa. La revisión más reciente de esta norma fue publicada en 2015.

Esta norma puede ser implementada en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande. Ha sido redactada por los mejores especialistas del mundo en el tema y proporciona una metodología para implementar la gestión de la seguridad de la información en una organización. También permite que una empresa sea certificada; es decir, que una entidad de certificación independiente confirma que la seguridad de la información ha sido implementada en esa organización en cumplimiento de la norma ISO 27001.
Esta norma ha pasado a ser la principal a nivel mundial para la seguridad de la información, y muchas empresas han certificado su cumplimiento.

Cómo funciona la ISO 27001

El objetivo principal es proteger la confidencialidad, integridad y disponibilidad de la información en una empresa. Esto se hace investigando qué problemas potenciales problemas podrían afectar la información (es decir, la evaluación de riesgos) y luego definir lo que es necesario hacer para evitar que tales problemas tengan lugar (esto es; mitigación o tratamiento del riesgo).

Por tanto, la filosofía principal de la norma se basa en la gestión de riesgos: investigar dónde están y luego tratarlos sistemáticamente.



Las medidas de seguridad (o controles) que se van a implementar se presentan, por lo general, bajo la forma de políticas, procedimientos e implementación técnica (por ejemplo, software y equipos); sin embargo, en la mayoría de los casos, las empresas ya tienen todo el hardware y software pero los utilizan de una forma no segura; por consiguiente, la mayor parte de la implementación de ISO 27001 estará relacionada con determinar las reglas organizacionales (por ejemplo, redacción de documentos) necesarias para prevenir violaciones de la seguridad.

Como este tipo de implementación demanda la gestión de múltiples políticas, procedimientos, personas, bienes, etc., dicha norma detalla cómo amalgamar todos estos elementos dentro del sistema de gestión de seguridad de la información.

Por eso, la gestión de la seguridad de la información no se acota solamente a la seguridad de TI (por ejemplo, cortafuegos, antivirus, etc.), sino que también tiene que ver con la gestión de procesos, de los recursos humanos, con la protección jurídica, la protección física, etcétera.

Por qué la ISO 27001 es importante para su empresa

Hay cuatro ventajas comerciales esenciales que una empresa puede obtener con la implementación de esta norma para la seguridad de la información:

1. Cumplir con los requerimientos legales. Cada vez hay más y más leyes, normativas y requerimientos contractuales relacionados con la seguridad de la información. La buena noticia es que una buena parte se pueden resolver implementando ISO 27001, ya que esta norma proporciona una metodología perfecta para cumplir con todos ellos.

2. Obtener una ventaja comercial. Si su empresa obtiene la certificación y sus competidores no, es posible que usted obtenga una ventaja sobre ellos ante los ojos de los clientes a los que les interesa mantener en forma segura su información.

3. Menores costos. La filosofía principal de la ISO 27001 es evitar que se produzcan incidentes de seguridad, y cada incidente, ya sea grande o pequeño, cuesta dinero; por tanto, al evitarlos, su empresa podrá ahorrar mucho dinero. Y lo mejor de todo es que la inversión en la ISO 27001 es mucho menor que el ahorro que se obtendrá.

4. Una mejor organización. En general, las empresas de rápido crecimiento no tienen tiempo para hacer una pausa y definir sus procesos y procedimientos; como consecuencia, muchas veces los empleados no saben qué hay que hacer, cuándo y quién debe hacerlo. La implementación de la ISO 27001 ayuda a resolver este tipo de situaciones, pues alienta a las empresas a escribir sus principales procesos (incluso los que no están relacionados con la seguridad), lo que les permite reducir el tiempo perdido de los empleados.

Dónde interviene la gestión de seguridad de la información en una empresa

Básicamente, la seguridad de la información es parte de la gestión global del riesgo en una empresa; hay aspectos que se superponen con la ciberseguridad, con la gestión de la continuidad del negocio y con la tecnología de la información:

Cómo es realmente ISO 27001

Esta norma se divide en once secciones más el anexo A; las secciones 0 a 3 son introductorias (y no son obligatorias para la implementación), mientras que las secciones 4 a 10 son obligatorias, lo que implica que una organización debe implementar todos sus requerimientos si quiere cumplir con la norma. Los controles del anexo A deben implementarse sólo si se determina que corresponden en la declaración de aplicabilidad.

De acuerdo con el Anexo SL de las Directivas ISO de la Organización Internacional para la Normalización, los títulos de las secciones de ISO 27001 son los mismos que los de la ISO 9001:2015 y en otras normas de gestión, lo que permite integrar más fácilmente estas normas.

Sección 0 – Introducción: explica el objetivo de ISO 27001 y su compatibilidad con otras normas de gestión.

Sección 1 – Alcance: indica que esta norma aplica en cualquier tipo de organización.

Sección 2 – Referencias normativas: hace referencia a la norma ISO 27000 como estándar en el que se proporcionan términos y definiciones.

Sección 3 – Términos y definiciones; de nuevo, hace referencia a la norma ISO 27000.

Sección 4 – Contexto de la organización: es parte de la fase de planificación del ciclo PDCA y define los requerimientos para comprender cuestiones externas e internas; también define las partes interesadas, sus requisitos y el alcance del SGSI.

Sección 5 – Liderazgo: es parte de la fase de planificación del ciclo PDCA y define las responsabilidades de la dirección, el establecimiento de roles y responsabilidades y el contenido de la política de alto nivel sobre seguridad de la información.

Sección 6 – Planificación: esta sección es parte de la fase de planificación del ciclo PDCA y define los requerimientos para la evaluación de riesgos, el tratamiento de riesgos, la declaración de aplicabilidad, el plan de tratamiento de riesgos y la determinación de los objetivos de seguridad de la información.

Sección 7 – Apoyo: esta sección es parte de la fase de planificación del ciclo PDCA y define los requerimientos sobre disponibilidad de recursos, competencias, concienciación, comunicación y control de documentos y registros.

Sección 8 – Funcionamiento: esta sección es parte de la fase de planificación del ciclo PDCA y define la implementación de la evaluación y el tratamiento de riesgos, como también los controles y demás procesos necesarios para cumplir los objetivos de seguridad de la información.

Sección 9 – Evaluación del desempeño: esta sección forma parte de la fase de revisión del ciclo PDCA y define los requerimientos para monitoreo, medición, análisis, evaluación, auditoría interna y revisión por parte de la dirección.

Sección 10 – Mejora: forma parte de la fase de mejora del ciclo PDCA y define los requerimientos para el tratamiento de no conformidades, correcciones, medidas correctivas y mejora continua.

Anexo A: Proporciona un catálogo de 114 controles (medidas de seguridad) distribuidos en 14 secciones (secciones A.5 a A.18).

Cómo implementar la ISO 27001
Para implementar la norma ISO 27001 en una empresa se deben seguir estos 16 pasos:

1. Obtener el apoyo de la dirección.
2. Utilizar una metodología para gestión de proyectos.
3. Definir el alcance del SGSI.
4. Redactar una política de alto nivel sobre seguridad de la información.
5. Definir la metodología de evaluación de riesgos.
6. Realizar la evaluación y el tratamiento de riesgos.
7. Redactar la declaración de aplicabilidad.
8. Redactar el plan de tratamiento de riesgos.
9. Definir la forma de medir la efectividad de los controles y del SGSI.
10. Implementar todos los controles y procedimientos necesarios.
11. Implementar programas de capacitación y concienciación.
12. Realizar todas las operaciones diarias establecidas en la documentación de su SGSI
13. Monitorear y medir el SGSI.
14. Realizar la auditoría interna.
15. Efectuar la revisión por parte de la dirección.
16. Implementar medidas correctivas.

Para obtener una explicación más detallada de estos pasos consulte la Lista de apoyo para implementación de la ISO 27001.

8 Documentación obligatoria

La ISO 27001 requiere que se confeccione la siguiente documentación:

- Alcance del SGSI (punto 4.3).
- Objetivos y política de seguridad de la información (puntos 5.2 y 6.2).
- Metodología de evaluación y tratamiento de riesgos (punto 6.1.2).
- Declaración de aplicabilidad (punto 6.1.3 d).
- Plan de tratamiento de riesgos (puntos 6.1.3 e y 6.2).
- Informe de evaluación de riesgos (punto 8.2).
- Definición de roles y responsabilidades de seguridad (puntos A.7.1.2 y A.13.2.4).
- Inventario de activos (punto A.8.1.1).
- Uso aceptable de los activos (punto A.8.1.3).

- Política de control de acceso (punto A.9.1.1).
- Procedimientos operativos para gestión de TI (punto A.12.1.1).
- Principios de ingeniería para sistema seguro (punto A.14.2.5).
- Política de seguridad para proveedores (punto A.15.1.1).
- Procedimiento para gestión de incidentes (punto A.16.1.5).
- Procedimientos para continuidad del negocio (punto A.17.1.2).
- Requisitos legales, normativos y contractuales (punto A.18.1.1).

Y estos son los registros obligatorios:

- Registros de capacitación, habilidades, experiencia y calificaciones (punto 7.2).
- Monitoreo y resultados de medición (punto 9.1).
- Programa de auditoría interna (punto 9.2).
- Resultados de auditorías internas (punto 9.2).
- Resultados de la revisión por parte de la dirección (punto 9.3).
- Resultados de medidas correctivas (punto 10.1).
- Registros sobre actividades de los usuarios, excepciones y eventos de seguridad (puntos A.12.4.1 y A.12.4.3).

Por supuesto, cualquier empresa puede confeccionar otros documentos de seguridad adicionales si lo considera necesario.

Cómo obtener la certificación

Hay dos tipos de certificados ISO 27001: para las organizaciones, y para las personas. Las organizaciones pueden obtener la certificación para demostrar que cumplen con todos los puntos obligatorios de la norma; las personas pueden hacer el curso y aprobar el examen para obtener el certificado.
Para obtener la certificación como organización, se debe implementar la norma tal como se explicó antes, y luego se debe aprobar la auditoría que realiza la entidad de certificación. La auditoría de certificación se realiza siguiendo estos pasos:

1. paso de la auditoría (revisión de documentación): los auditores revisarán toda la documentación.

2. paso de la auditoría (auditoría principal): los auditores efectuarán la auditoría in situ para comprobar si todas las actividades de una empresa cumplen con ISO 27001 y con la documentación del SGSI.

Visitas de supervisión: después de que se emitió el certificado, y durante su vigencia de tres años, los auditores verificarán si la empresa mantiene su SGSI.
Las personas pueden asistir a diversos cursos para obtener certificados. Los más populares son los siguientes:

1. Curso de auditor líder en ISO 27001: en este curso de cinco días se indica cómo realizar auditorías de certificación y está orientado a auditores y consultores.
2. Curso de implementador principal de ISO 27001: en cinco días se precisa cómo implementar la norma y está orientado a profesionales y consultores en seguridad de la información.
3. Curso de auditor interno en ISO 27001: en dos o tres días se ofrecen los conceptos básicos de la norma y se indica cómo llevar a cabo una auditoría interna; está orientado a principiantes en este tema y a auditores internos.

Otras normas relacionadas con seguridad de la información

1. ISO 27002: proporciona directrices para la implementación de los controles indicados en la ISO 27001. ISO 27001 especifica 114 controles que pueden ser utilizados para disminuir los riesgos de seguridad, y la norma ISO 27002 puede ser bastante útil ya que proporciona más información sobre cómo implementar esos controles. A la ISO 27002 se la conocía como ISO/IEC 17799 y surgió de la norma británica BS 7799-1.

2. ISO 27004: ofrece directrices para la medición de la seguridad de la información; se acopla bien con la ISO 27001, pues indica cómo determinar si el SGSI ha alcanzado los objetivos.

3. ISO 27005: proporciona directrices para la gestión de riesgos de seguridad de información. Es un muy buen complemento para la ISO 27001, ya que brinda más información sobre cómo llevar a cabo la evaluación y el tratamiento de riesgos, probablemente la etapa más difícil de la implementación. La ISO 27005 deriva de la norma británica BS 7799-3.

4. ISO 22301: define los requerimientos para los sistemas de gestión de continuidad del negocio, se adapta muy bien con la ISO 27001 porque el punto A.17 de esta última requiere la implementación de la continuidad del negocio, aunque no proporciona demasiada información.

5. ISO 9001: define los requerimientos para los sistemas de gestión de calidad. Aunque a primera vista la gestión de calidad y la gestión de seguridad de la información no tienen mucho en común, lo cierto es que aproximadamente el 25% de los requisitos de la ISO 27001 y de la ISO 9001 son los mismos: control de documentos, auditoría interna, revisión por parte de la dirección, medidas correctivas, definición de objetivos y gestión de competencias. Esto quiere decir que si una empresa ha implementado la ISO 9001 le resultará mucho más sencillo implementar la ISO 27001.

Cabe subrayar que la función que tenemos en MUNDO CP es apoyar a los profesionales asesores de las empresas en el cumplimiento de obligaciones en el área de seguridad social y laboral, pero también secundar a nuestros socios de negocios, por lo que además de ofrecer artículos como este buscamos ampliar los contadores públicos.

Asímismo, un servidor junto con Treblink Consultores SC, orientamos en el cumplimiento de las normas oficiales mexicanas de seguridad y salud en el trabajo; y las normas ISO.

L.C.P. Martin Ernesto Quintero Garcia
Especialista en Seguridad Social
RMA Consultores Profesionales SC mquintero@rma.com.mx

Con la Colaboración de
C.P. Horacio Flores Romo Chávez
Socio -
Consultor Treblink Consultores SC
treblink023@gmail.com