ANEXO A: Síntesis del estándar ISO/IEC 27001:2005[J]

A continuación se presenta la ISO/IEC 27001:2005[J] a manera de resumen con el objetivo de entender el alcance y contenido de la misma y comprender el trabajo requerido para aplicar la misma en una empresa.

0. Introducción:

0.1. Generalidades:

Este estándar provee un modelo para el establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora del SGSI. La adopción del SGSI debe ser una decisión estratégica por tener un enfoque hacia las necesidades y objetivos de la empresa.

0.2. Enfoque basado en procesos:

Este estándar adopta el modelo PHVA "Planificar-Hacer-Verificar-Actuar" (en inglés PDCA "Plan-Do-Check-Act") en los procesos del SGSI. A continuación, se muestra la figura A-01 del modelo PHVA aplicado a los procesos de SGSI y alineado a los puntos de referencia en la norma ISO/IEC: 27001:2005[J]:

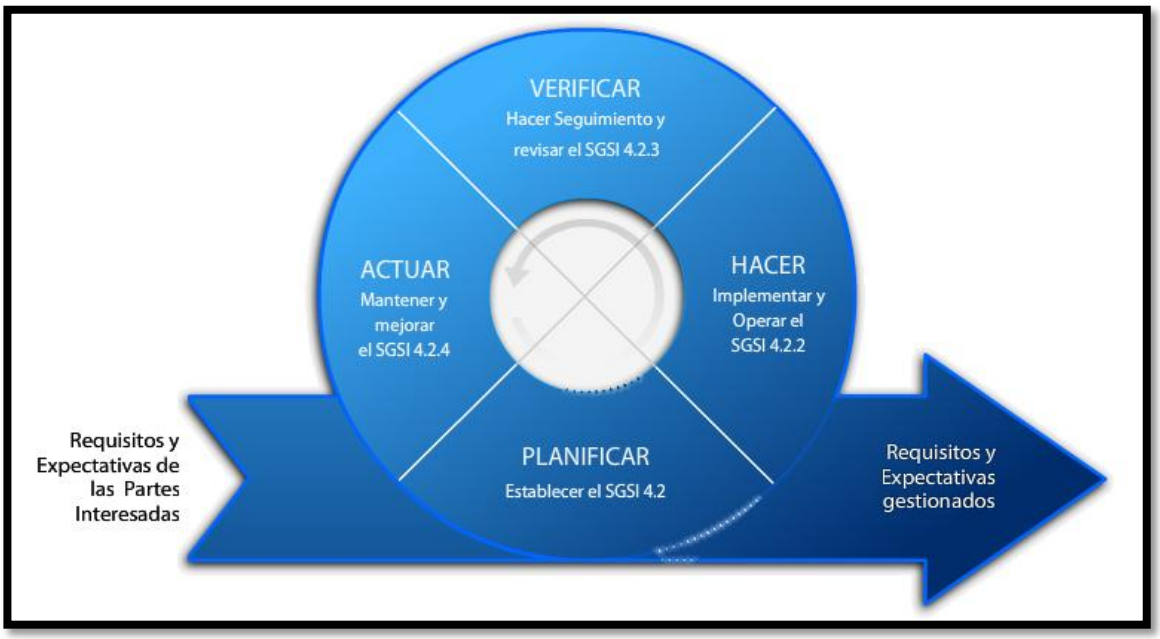

Figura A-01 Ciclo PHVA

0.3. Compatibilidad con otros Sistemas de Gestión:

La norma está alineada con la ISO 9001:2000 y la ISO 14001:2004 que apoyan en la implementación y operación de los sistemas de gestión de una empresa integrados con el SGSI.

1. Alcance: Especificación del objetivo del estándar, su aplicación y tratamiento de exclusiones.

1.1. Generalidades

La ISO/IEC 27001:2005[J] especifica los requisitos para establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar un SGSI documentado, así como los requisitos para la implementación de controles de seguridad de la información, según las necesidades de la empresa.

1.2. Aplicación de la ISO/IEC 27001:2005[J]

Los requerimientos en esta norma son genéricos y aplicables a todo tipo de empresas. Para el cumplimiento de esta norma, no es aceptable la exclusión de los requisitos obligatorios en las cláusulas 4 (Elementos del SGSI), 5 (Responsabilidades de la Gerencia), 6 (Auditorías Internas del SGSI), 7 (Revisiones del SGSI) y 8 (Mejora Continua del SGSI). Para el resto de puntos contenidos en el SGSI, toda exclusión de controles debe justificarse y evidenciar que los riesgos han sido asumidos por los responsables y que la capacidad para ofrecer seguridad a la información no ha sido afectada.

2. Referencias normativas: Para la aplicación de la norma ISO/IEC 27001:2005[J], se debe hacer referencia a la norma directamente relacionada ISO/IEC 17799[B]:2005, teniendo en cuenta su última versión y la siguiente forma:

> *"ISO/IEC 17799:200x, Information technology. Security techniques. Code of practice for information security management"*

3. Términos y definiciones: Descripción de los términos más usados en la norma en alineación a otras normas similares, a fin de evitar interpretaciones incorrectas. Aceptación del riesgo: decisión de asumir un riesgo.
   - Activo: cualquier cosa que tenga valor para la empresa.
   - Análisis de riesgo: uso sistemático de la información para identificar fuentes y estimar riesgos.

- Confidencialidad: propiedad que asegura que la información no pueda estar disponible ni pueda ser descubierta por personas, entidades o procesos no autorizados.
- Declaración de aplicabilidad: documento que describe los objetivos de control para el SGSI de la empresa.
- Disponibilidad: propiedad que garantiza que la información sea accesible y usable bajo demanda de una entidad autorizada.
- Evaluación del riesgo: proceso de comparar el riesgo estimado contra criterios definidos para determinar la importancia del mismo.
- Eventos de seguridad de la información: Condiciones en un sistema, servicio o red, que indican posibles violaciones del SGSI o fallo de las medidas de contingencia.
- Gestión del riesgo: Actividades coordinadas para dirigir y controlar a una empresa en relación al riesgo.
- Incidente de seguridad de la información: eventos no deseados que tienen una alta probabilidad de comprometer las operaciones de la empresa y amenazar la seguridad de la información.
- Integridad: propiedad de salvaguardar la exactitud y estado de los activos de información.
- Riesgo residual: riesgo remanente luego de su tratamiento.
- Seguridad de la información: preservación de la confidencialidad, integridad y disponibilidad de la información, además de otras propiedades como autenticidad, trazabilidad, no repudio y fiabilidad.
- Sistema de gestión de la seguridad de la información - SGSI: parte del sistema de gestión de la empresa, basado en un enfoque hacia riesgos empresariales cuyo fin es establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar la seguridad de la información.
- Tratamiento de riesgo: proceso selección e implementación de medidas (controles) para reducir el riesgo.
- Valoración de riesgo: procesos de análisis y evaluación de riesgo.

4. Elementos del Sistema de Gestión de la Seguridad de la Información – SGSI:

4.1. Requisitos generales:

Como se ha mencionado a lo largo de este resumen, la empresa establecerá, implementará, operará, hará seguimiento, revisará, mantendrá y mejorará un *SGSI basado en el modelo PHVA* indicado en el punto 0.2., a continuación se presentan los requisitos para lograr este objetivo:

4.2. Establecimiento y gestión del SGSI

4.2.1. Establecimiento del SGSI: En este apartado la norma indica lo que debería hacer la empresa para establecer un SGSI:

a. Definir el alcance y límites del SGSI
b. Definir una política de SGSI y hacer aprobar por la gerencia.
c. Definir un enfoque organizacional para la gestión de riesgos mediante:
   - la identificación de una metodología para la valoración de riesgos y
   - el desarrollo de criterios y niveles de aceptación de riesgos.
d. Identificar los riesgos
e. Analizar y evaluar riesgos
f. Seleccionar controles y objetivos de control
g. Obtener aprobación de la gerencia sobre los riesgos residuales propuestos.
h. Elaborar una declaración de aplicabilidad

4.2.2. Implementación y operación del SGSI: En este apartado la norma indica lo que debería hacer la empresa para implementar y operar un SGSI:

a. Formular un plan para el tratamiento de riesgos
b. Implementar el plan para el tratamiento de riesgos para lograr los objetivos de control identificados, considerando la financiación y asignación de funciones y responsabilidades.
c. Implementar controles en el punto 4.2.1. f. para cumplir los objetivos de control.
d. Definir cómo medir la eficacia de los controles seleccionados. Estos resultados permitirán a la gerencia determinar el cumplimiento de los objetivos de control planificados.
e. Implementar programas de capacitación y toma de conciencia al personal (5.2.2.)
f. Gestionar la operación y recursos (5.2.) del SGSI.
g. Implementar procedimientos y otros controles para detectar y responder a los incidentes de seguridad (4.2.3.)

4.2.3. Seguimiento y revisión del SGSI: En este apartado la norma indica lo que debería hacer la empresa para hacer el seguimiento y revisiones a su SGSI:

a. Ejecutar procedimientos de seguimiento y revisión
b. Realizar revisiones regulares de la eficacia del SGSI

c. Medir la eficacia de los controles para verificar el cumplimiento de los requisitos de seguridad.
d. Revisar la valoración de riesgos en los periodos identificados y nivel de riesgo residual.
e. Realizar auditorías internas del SGSI (6).
f. Revisar regularmente el SGSI por parte de la gerencia para asegurar que el alcance siga siendo suficiente y para identificar mejoras.
g. Actualizar planes de seguridad
h. Registrar acciones y eventos que podrían tener impacto en el desempeño del SGSI.

4.2.4. Mantenimiento y mejora del SGSI: En este apartado la norma indica lo que debería hacer la empresa de manera regular para dar el mantenimiento y mejora continua a su SGSI:

a. Implementar las mejoras identificadas en el SGSI.
b. Ejecutar acciones correctivas y preventivas (8.2. y 8.3). Aplicar las lecciones aprendidas.
c. Comunicar las acciones y mejoras a las partes interesadas con un nivel de detalle según las circunstancias y llegando a acuerdos en donde sea pertinente.
d. Asegurar que las mejoras logren los objetivos previstos.

4.3. Requisitos de la documentación

4.3.1. Generalidades

El SGSI debe tener registros trazables (en cualquier tipo de medio) de las decisiones de la gerencia con resultados reproducibles. Es importante poder demostrar la relación entre los controles seleccionados y los resultados de la valoración y tratamiento de riesgos y con la política y objetivos del SGSI. Según la norma, la documentación debe incluir:

a. Alcance del SGSI (4.2.1. a.)
b. Declaraciones de la política y objetivos del SGSI (4.2.1. b.)
c. Descripción de la metodología de valoración de riesgos (4.2.1. c.)
d. Informe de valoración de riesgos (4.2.1. c. – g.)
e. Plan de tratamiento de riesgos (4.2.2. b.)
f. Procedimientos documentados (establecidos, documentados, implementados y mantenidos) para asegurar la eficacia de la planificación, operación y control de sus procesos de seguridad de información (4.2.3 a.)

g. Registros exigidos por la norma como tal (4.3.3.)
h. Declaración de aplicabilidad de la documentación.

4.3.2. Control de documentos

Los documentos requeridos por el SGSI deben ser protegidos y controlados. Se debe documentar un procedimiento para definir las acciones de gestión para: aprobar, revisar y actualizar documentos; asegurar que las últimas versiones estén disponibles y que sean legibles e identificables. Se deben aplicar procedimientos pertinentes para la clasificación, control de transferencia, distribución, almacenamiento y disposición final de los documentos y asegurar que los documentos externos también sean identificados. Prevenir el uso de documentos obsoletos e identificar a aquellos que siendo obsoletos se guarden por algún propósito.

4.3.3. Control de registros

La norma exige el establecimiento y mantenimiento de registros para evidenciar el desempeño, cumplimiento y operación eficaz de los requisitos del SGSI (por ejemplo con bitácoras de visitas, informes de auditorías y formatos de autorización de accesos) (4.2.). Se deben documentar e implementar controles para la identificación, almacenamiento, protección, recuperación, tiempo de retención y disposición de registros.

5. Responsabilidades de la Gerencia: Descripción del compromiso de la empresa con el SGSI, gestión y provisión de recursos y concienciación, formación y capacitación del personal.

5.1. Compromiso de la gerencia

La gerencia debe evidenciar su compromiso con el establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora del SGSI a través del establecimiento de la política, objetivos y planes del SGSI y los roles y responsabilidades para la seguridad de la información. Además, debe comunicar la importancia del cumplimiento de los objetivos de seguridad y de la política de seguridad, responsabilidades legales y la necesidad de una continua mejora al personal de la empresa y proporcionar los recursos para poder establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar el SGSI (5.2.1), decidir los criterios de aceptación de riesgos y sus niveles aceptables y asegurar la realización de auditorías internas y revisiones al SGSI (7.).

5.2. Gestión de recursos

5.2.1. Provisión de recursos

En este apartado la norma indica lo que debería hacer la empresa para determinar y suministrar los recursos necesarios para establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar un SGSI, asegurar que los procedimientos de seguridad de información brinden apoyo a los requisitos del negocio, identificar y atender los requisitos legales, reglamentarios y obligaciones contractuales, mantener la seguridad mediante la aplicación de los controles implementados, llevar a cabo revisiones y ejecutar acciones según los resultados de los mismos y mejorar la eficacia del SGSI en donde sea requerido.

5.2.2. Formación, conocimiento y competencia

La empresa tiene que asegurar que todo el personal a quien se asignen responsabilidades en el SGSI tenga conciencia de la importancia de sus actividades para la seguridad de la información y contribución a los logros de los objetivos del SGSI y sea competente y en capacidad de ejecutar las tareas requeridas mediante:

a. La determinación de competencias necesarias para el personal que trabaja con el SGSI.
b. El suministro de formación u otras acciones (por ejemplo contrataciones de personal competente) para satisfacer las necesidades.
c. La evaluación de la eficacia de acciones emprendidas
d. Mantenimiento de los registros de formación, habilidades, experiencia y calificaciones (4.3.3.)

6. Auditorías internas del SGSI: Proporciona directrices sobre cómo realizar las auditorías internas de control y cumplimiento.

   La empresa debe realizar auditorías internas programadas al SGSI para determinar si los objetivos de control, controles, procesos y procedimientos cumplen con los requisitos de la norma y de la legislación o reglamentación, están implementados y mantenidos de manera eficiente y tienen un desempeño esperado. Se deben documentar procedimientos con las responsabilidades y requisitos para la planificación y realización de las auditorías.
7. Revisiones al SGSI: Proporciona guías sobre cómo gestionar el proceso periódico de revisión del SGSI por parte de la dirección.

7.1. Generalidades

La gerencia debe revisar el SGSI al menos una vez al año para asegurar su efectividad continua. En la revisión de sebe hacer una evaluación de oportunidades de mejora y cambios necesarios al SGSI. Los resultados de la revisión deben documentarse (4.3.3.)

7.2. Entradas o datos iniciales para la revisión

a. Resultados de las auditorías y revisiones al SGSI
b. Retroalimentación de las partes interesadas
c. Técnicas, productos o procedimientos que se usan en la empresa para mejorar el desempeño del SGSI
d. Estado de las acciones correctivas y preventivas
e. Vulnerabilidades o amenazas no tratadas adecuadamente en la valoración previa de riesgos.
f. Resultados de mediciones de eficacia
g. Acciones de seguimientos resultantes de revisiones de la gerencia
h. Cambios al SGSI
i. Recomendaciones de mejora

7.3. Salidas o resultados de la revisión

a. Mejora de la eficacia del SGSI
b. Actualización de la evaluación de riesgos y del plan de tratamiento de riesgos.
c. Modificación de procedimientos y controles que afectan la seguridad de la información, según sea necesario.
d. Recursos necesarios
e. Mejora a la manera en que se mide la eficacia de los controles.

8. Mejora continua del SGSI: Descripción de los mecanismos de mejora continua, acciones correctivas y acciones preventivas.

8.1. Mejora continua

La empresa debe mejorar continuamente la eficacia del SGSI a través del uso de la política de seguridad de información, los resultados de las auditorías, el análisis de eventos a los cuales se han dado seguimiento, las acciones preventivas y correctivas y revisiones de la gerencia.

8.2. Acción correctiva

La empresa debe emprender acciones para eliminar las causas del incumplimiento de los requisitos del SGSI mediante un procedimiento documentado en la cual se definen requisitos para identificar los incumplimientos y sus causas, evaluar la necesidad de las acciones, determinar e implementar la acción correctiva necesaria, registrar los resultados de la acción (4.3.3) y revisar la acción correctiva tomada.

8.3. Acción preventiva

La empresa debe emprender acciones para eliminar las causas potenciales del incumplimiento de los requisitos del SGSI, tiene que identificar los cambios en los riesgos mediante un procedimiento documentado en el cual se definen requisitos para identificar los incumplimientos potenciales y sus causas, evaluar la necesidad de las acciones para impedir que ocurra el incumplimiento, determinar e implementar la acción preventiva necesaria, registrar los resultados de la acción (4.3.3) y revisar la acción preventiva tomada.

El anexo A de esta norma propone un cuadro detallado de los controles, los cuales quedan agrupados y numerados de la siguiente forma:

A.5 Política de seguridad
A.6 Organización de la información de seguridad
A.7 Administración de recursos
A.8 Seguridad de los recursos humanos
A.9 Seguridad física y del entorno
A.10 Administración de las comunicaciones y operaciones
A.11 Control de accesos
A.12 Adquisición de sistemas de información, desarrollo y mantenimiento
A.13 Administración de los incidentes de seguridad
A.14 Administración de la continuidad de negocio
A.15 Cumplimiento (legales, de estándares, técnicas y auditorías)

El anexo B, que es informativo, a su vez proporciona una breve guía de los principios de OECD (guía de administración de riesgos de sistemas de información y redes - París, Julio del 2002, "www.oecd.org") y su correspondencia con el modelo PDCA.

Por último el Anexo C, también informativo, resume la correspondencia entre esta norma y los estándares ISO 9001:2000 y el ISO 14001:2004