

ESTÁNDARES DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN


1 LA ORGANIZACIÓN ISO

ISO (Organización Internacional de Estándares) es una organización especializada en el desarrollo y difusión de los estándares a nivel mundial.

Los miembros de ISO, son organismos nacionales que participan en el desarrollo de Normas Internacionales a través de comités técnicos establecidos para tratar con los campos particulares de actividad técnica. Los comités técnicos de ISO colaboran en los campos de interés mutuo con la IEC (International Electrotechnical Commission), la organización que a nivel mundial prepara y publica estándares en el campo de la electro tecnología. En el campo de tecnología de información, ISO e IEC han establecido unir un comité técnico, ISO/IEC JTC 1 (Join Technical Committee N°1).

Los borradores de estas Normas Internacionales son enviados a los organismos de las diferentes naciones para su votación. La publicación, ya como una Norma Internacional, requiere la aprobación de por lo menos el 75% de los organismos nacionales que emiten su voto.

2 LA FAMILIA DE LAS NORMAS ISO

A semejanza de otras normas ISO, la 27000  es realmente una serie de estándares.

ISO/IEC27000 Sistemas de Gestión de Seguridad de la Información, Generalidades y vocabulario, en la que se recogen los términos y conceptos relacionados con la seguridad de la información, una visión general de la familia de estándares de esta área, una introducción a los SGSI, y una descripción del ciclo de mejora continua.

ISO/IEC 27001, Sistemas de Gestión de la Seguridad de la Información (SGSI). Requisitos. Esta es la norma fundamental de la familia, ya que contiene los requerimientos del sistema de gestión de seguridad de la información y es la norma con arreglo a la cual serán certificados los SGSI de las organizaciones que lo deseen.

- ISO/IEC27002, Tecnología de la Información. Código de buenas prácticas para la Gestión de la Seguridad de la Información, publicada en el año 2013. Esta guía de buenas prácticas describe los objetivos de control y controles recomendables en cuanto a seguridad de la información.

- ISO/IEC27003. Guía de implementación de SGSI e información acerca del uso del modelo PDCA y de los requerimientos de sus diferentes fases

- ISO27004: Estándar para la medición de la efectividad de la implantación de un SGSI y de los controles relacionados.

- ISO/IEC27005 Gestión del Riesgo en la Seguridad de la Información, publicada en el año 2008. Esta norma al pertenecer a la familia de las Normas 27000, se ajusta a las necesidades de las organizaciones que pretende realizar su análisis de riesgos en este ámbito y cumplir con los requisitos de la Norma ISO 27001.

ING. FERNANDO CARPENTIERI
SISTEMAS DE GESTIÓN
CAPACITACIÓN Y ASISTENCIA TÉCNICA

- ISO/IEC27006. Requisitos para las entidades que suministran servicios de auditoría y certificación de sistemas de gestión de seguridad de la información. Recoge los criterios mediante los cuales una organización se puede acreditar para realizar esos servicios.
- ISO/IEC27007. Guía para la realización de las auditorías de un SGSI.

Entre otras.

3 ISO 27001

La norma ISO/IEC 27001 especifica los requisitos para establecer, implantar, documentar y evaluar un Sistema de Gestión de la Seguridad de la Información (en adelante SGSI) de acuerdo a la Norma ISO 27002 dentro del contexto de los riesgos identificados por la Organización.

Los requisitos de esta Norma aplican a todo tipo de organizaciones, independientemente de su tipo, tamaño o área de actividad.

Asimismo, está basada en un enfoque por procesos y en la mejora continua, por lo tanto, es perfectamente compatible e integrable con el resto de sistemas de gestión que ya existan en la organización.

La Norma asume que la organización identifica y administra cualquier tipo de actividad para funcionar eficientemente. Cualquier actividad que emplea recursos y es administrada para transformar entradas en salidas, puede ser considerada como un "proceso". A menudo, estas salidas son aprovechadas nuevamente como entradas, generando una realimentación de los mismos. Estos procesos se someten a revisiones para detectar fallos e identificar mejoras, por lo que se encuentran dentro de un proceso de mejora continua.

La Norma recoge los componentes del SGSI, es decir, en qué consiste la parte documental del sistema:

- qué documentos mínimos deben formar parte del SGSI,
- cómo se deben crear, gestionar y mantener y cuáles son los registros que permitirán evidenciar el buen funcionamiento del sistema.
- Cómo se debe diseñar e implantar el SGSI.
- Define los controles de seguridad a considerar. Se requiere que se escojan los controles del Anexo A, que recoge todos los controles detallados en la Norma ISO/IEC 27002.
- Cómo debe realizarse la revisión y mejora del SGSI.
- La ISO 27001 adopta un proceso para establecer, implementar, operar, monitorizar, revisar, mantener y mejorar el SGSI en una organización.

4. ANÁLISIS DE LOS REQUISITOS GENERALES DE ISO 27001

La norma está dividida en siete capítulos que recogen requisitos (capítulos 4 al 10). Su análisis se establece a continuación

4. Contexto de la organización.

Este elemento está centrado en identificar quienes son los clientes o beneficiarios del SGSI. Para ello, la organización se debe plantear diferentes puntos de vista desde los que ver el porqué de las necesidades de seguridad y cuáles son los requisitos a garantizar. Todo ello se concreta en las siguientes subcláusulas.

4.1 Entender la organización y su contexto.

Para todo SGSI es vital entender nuestro modelo de negocio y nuestro entorno. Considerar todo aquello que puede condicionar el lograr los resultados de nuestro SGSI.

4.2 Entender las necesidades y expectativas de las partes interesadas

También es crítico identificar quienes son nuestras partes interesadas internas y cuáles son sus necesidades respecto a la seguridad. En este sentido el alcance del SGSI puede o no cubrir todos los procesos de negocio de la Organización y en el caso de ser sólo una parte, tendrá como partes interesadas a otras áreas que serán “clientes” de la seguridad.

4.3 Determinar el alcance del SGSI.

Con todas las reflexiones anteriores en Este capítulo se determina la creación del primero de los documentos que constituyen el SGSI, “el alcance del sistema”. Se deben establecer los límites del SGSI en el alcance que tiene que ser expresado en términos de:

- 1) asuntos internos y externos considerados en 4.1
- 2) requisitos identificados de las necesidades establecidas en 4.2
- 3) interfaces y dependencias entre las actividades realizada por la organización y las que son realizadas por otras organizaciones.

5 Liderazgo

Este capítulo reúne los requisitos para garantizar que la puesta en marcha del SGSI efectivamente es un proceso estratégico y establece las directrices de gestión de alto nivel que deben motivar el funcionamiento del sistema.

5.1 Liderazgo y compromiso

La alta dirección debe demostrar liderazgo y compromiso con el SGSI sobre todo de las siguientes formas:

- 1) asegurando que los objetivos se establecen y son compatibles con la dirección estratégica de la organización.
- 2) garantizando que sí que se integra el SGSI con los procesos de la organización y proporcionando los recursos necesarios.
- 3) asegurando que el SGSI logra los resultados esperados.

En este apartado ya se empieza a ver uno de los cimientos del SGSI, que los resultados muestren que se alcanzan los objetivos.

5.2 Política

En Este capítulo se formaliza ese compromiso de la Dirección obligando a documentar el segundo de los documentos que constituyen el SGSI, “la política de seguridad”. Al menos, debe establecer directrices de gestión respecto a:

- 1) ser adecuada al propósito de la organización.
- 2) incluir objetivos o proporcionar un marco para establecerlos.
- 3) incluir compromisos de satisfacer los requisitos aplicables y garantizar la mejora continua.

5.3 Roles de la organización, responsabilidades y autoridad.

La componente organizativa tampoco se descuida y todos los miembros activos que forman parte del funcionamiento del SGSI deben tener asignadas unas claras tareas y responsabilidades.

Las tareas del SGSI se estratifican a diferentes niveles del organigrama y habrá personal más vinculado con la gestión del propio sistema y el soporte de los procesos propios como el control de la documentación, la mejora continua o la medición y otro personal más centrado en las tareas operativas de administración y operación de las medidas de seguridad que implantan controles del anexo A de ISO 27001.

Para todos ellos, en este punto se determina que:

- A) Se deben asignar responsabilidades y autoridad para garantizar que el SGSI es conforme al estándar.
- B) Informar a la dirección del rendimiento del  SGSI.

6. Planificación

Este capítulo secuenciar los pasos para la creación del SGSI en donde es una tarea clave y principal para la toma de decisiones el proceso de identificación y análisis del riesgo.

6.1. Acciones para dirigir los riesgos y oportunidades.

La planificación del SGSI está condicionada por los objetivos propios de la Organización, los requisitos identificados en el capítulo 4 y el propio análisis de los riesgos. La organización debe planificar el SGSI para determinar los riesgos y oportunidades que le permita:

- A) asegurar que el SGSI logra los resultados.
- B) prevenir o reducir los efectos no deseados.
- C) lograr la mejora continua.

Es importante el lograr el cumplimiento de las metas como un factor determinante para valorar la salud del SGSI.

En relación al proceso de identificación y análisis del riesgo destacan los siguientes aspectos:

- 1) Se deben identificar los riesgos estimando las posibles pérdidas potenciales de confidencialidad, integridad y disponibilidad dentro del alcance del SGSI.
- 2) Identificar los propietarios de dichos riesgos.
- 3) Analizar las potenciales consecuencias en el caso de que los riesgos se materializaran ya determinan unas probabilidades realistas definiendo unos niveles de riesgo.

ING. FERNANDO CARPENTIERI
SISTEMAS DE GESTIÓN
CAPACITACIÓN Y ASISTENCIA TÉCNICA

- 4) Evaluar los riesgos identificados comparando los resultados obtenidos con los criterios de nivel de riesgo aceptable preestablecidos.
- 5) Priorizar en un plan las acciones a realizar para reconducir la situación.

En relación al proceso de tratamiento del riesgo destacan los siguientes aspectos en relación al contenido del plan:

- 1) Seleccionar la opción del riesgo más adecuada (Aceptar, reducir, evitar o transferir).
- 2) Determinar que controles son necesarios según las opciones de riesgo establecidas.
- 3) Comparar esos controles con los del anexo A para no olvidar ni omitir ninguno.
- 4) Realizar una declaración de aplicabilidad
- 5) Elaborar una planificación de implantación.
- 6) Obtener de los propietarios del riesgo una aprobación formal de los niveles de riesgo residuales, es decir, contar con el visto bueno de todos aquellos responsables que podrían tener problemas de seguridad respecto del conjunto de acciones que se quieren poner en marcha para que las consideren suficientes o para que decidan incluir más mecanismos de protección.

6.2 Objetivos y planes para lograrlos.

Los objetivos deben estar formalizados. En este sentido, la organización deberá establecer objetivos según funciones y niveles de forma que sean coherentes con la política de seguridad, sean medibles, tengan en cuenta los requisitos y necesidades del SGSI así como los resultados del análisis de riesgos.

Para estos objetivos se deberá determinar:

- que se tendrá que lograr
- que recursos serán necesarios
- quién será responsable del seguimiento del objetivo
- cuando se darán por logrados
- cómo se medirán los resultados.



El funcionamiento del SGSI debe estar guiado por un cuadro general de indicadores que verifican el estado de situación de los objetivos y nos indican su cumplimiento, su tendencia y los márgenes de reacción cuando las cosas no vayan bien.

7. Soporte

Este capítulo establece qué medios serán necesarios en la puesta en marcha del SGSI. En este sentido además de identificar las necesidades materiales se insiste también en la importancia de las personas y de sus capacidades técnicas siendo necesaria la formación y la concienciación para garantizar que son las adecuadas.

Además, se especifican los requisitos generales que debe garantizar el sistema en relación a la documentación que forma parte del mismo y al proceso de gestión respecto a los cambios o actualizaciones necesarios para ir manteniéndolo vigente.

7.1 Recursos

Cómo es obvio, una decisión estratégica de este calado debe contar con los recursos necesarios para lograr el buen funcionamiento del SGSI. Los ajustes presupuestarios podrán

ING. FERNANDO CARPENTIERI

SISTEMAS DE GESTIÓN CAPACITACIÓN Y ASISTENCIA TÉCNICA

influir en las posibles inversiones a realizar y condicionarán la gestión de riesgos de la organización, pero en cualquier caso, siempre hay unos mínimos que habrá que asumir como son la dedicación del personal que vigila y opera el SGSI.

7.2 Competencias.

En relación al factor humano, el equipo de personas que de soporte al SGSI debe tener un adecuado nivel de conocimiento o disponer de los recursos para hacer que los logren. Además, debe quedar evidencia de este proceso de capacitación.

7.3 Toma de conciencia

El personal que trabaja dentro del alcance del SGSI también debe ser consciente de la política de seguridad, de su contribución a la efectividad del sistema y de sus implicaciones en la resolución de no conformidades.

7.4 Comunicación.

Este apartado formaliza las vías de comunicación dentro del SGSI y determina que deberán identificarse las necesidades internas y externas en materia de comunicación sobre la seguridad de la información estableciendo:

- A) que debe comunicar.
- B) cuando debe hacerse.
- C) a quien debe hacerse.
- D) quien comunicará.
- E) como la comunicación será transportada o que medios se utilizarán.

Estos aspectos son extremadamente relevantes cuando ocurren incidentes de seguridad donde la agilidad de los procesos de notificación puede minimizar el tiempo de respuesta y reducir los posibles daños.

7.5 Documentación.

En este elemento se definen los requisitos generales para el control de la documentación del sistema. Los factores que pueden condicionar el nivel de documentación podrían ser:

- a) su tamaño, tipo de actividades, productos y servicios.
- b) la complejidad de sus procesos y sus interacciones.
- c) la competencia de las personas.

En líneas generales, el proceso de gestión de documentación no cambia mucho respecto a los requisitos anteriores. Se tiene que la documentación:

- a) se identifica y describe.
- b) identifica el formato y el medio.
- c) es revisada para mantenerla en vigor y actualizada.

La documentación requerida por el SGSI deberá estar controlada para asegurar:

- a) está accesible y adecuada para su uso cuándo y dónde sea necesario.
- b) está adecuadamente protegida.
- c) se controlan los cambios.
- d) se garantizan los periodos de retención y conservación.

Además, deberá definirse como se gestiona el ciclo de vida de la documentación: creación, distribución, acceso, uso, almacenamiento y destrucción.

La documentación de origen externo que se determine necesaria para la planificación y operación del SGSI deberá también ser identificada, apropiada y controlada.

8. Operación.

Este elemento determina cómo se garantiza el funcionamiento del SGSI una vez ha completado su fase de construcción y entra en los diferentes ciclos PDCA en años sucesivos.

8.1. Planificación operativa y control.

Para ello, en este elemento se determina que la organización deberá planificar, implementar y controlar los procesos necesarios para garantizar los requisitos e implementar las acciones necesarias para la gestión del riesgo (6.1).

La organización deberá implementar los planes para alcanzar los objetivos de seguridad propuestos (6.2).

La organización mantendrá registro para tener la necesaria confianza de que los procesos del SGSI siguen siendo bien gestionados según lo planificado o debe modificar controles planificados y revisar las consecuencias de los cambios no intencionados para mitigar cualquier efecto adverso cuando sea necesario.

La organización deberá asegurar que los procesos externalizados están definidos y controlados.

8.2. Análisis del riesgo.



El análisis de riesgos es un proceso recurrente que debe ajustar las decisiones de la organización o plantear cambiar el “apetito de riesgo” según se vayan logrando resultados que manifiesten el control de los riesgos que se están ya gestionando. Para ello, debe realizarse el proceso de identificación del riesgo a intervalos planificados o cuando se planteen u ocurran cambios significativos, tomando acciones según los criterios de aceptación del riesgo (6.1.2.a)

8.3. Tratamiento del riesgo.

La organización estará implantando el plan de tratamiento del riesgo. Conforme se logren ciertos hitos, se irán modificando los criterios de aceptación del riesgo y eso provocará que año tras año los planes se vayan también actualizando para reflejar la nueva toma de decisiones. Por tanto, la gestión de la seguridad implica la ejecución continuada del plan de tratamiento que año tras año se debe también revisar.

9. Evaluación del rendimiento.

Si en el elemento 6.2 Objetivos se definió cuáles son los beneficios esperados del funcionamiento del SGSI, en este elemento 9 se establece cómo se analizará si dichos objetivos se están o no cumpliendo.

9.1. Monitorización, medición, análisis y evaluación.

Para que la organización pueda evaluar el rendimiento y la efectividad del SGSI, se tiene que concretar y determinar:

- a. que necesita ser monitorizando y medido, incluyendo los procesos de seguridad y controles.

ING. FERNANDO CARPENTIERI

SISTEMAS DE GESTIÓN CAPACITACIÓN Y ASISTENCIA TÉCNICA

- b. los métodos para monitorizar, medir, analizar y evaluar, cuando sea aplicable, para asegurar unos resultados adecuados.
- c. cuando las monitorizaciones y mediciones deberán ser realizadas.
- d. quién deberá monitorizar y medir.
- e. cuando los resultados de la monitorización y medición deberán ser analizados y evaluados (rangos de normalidad y anomalía)
- f. quien analizara y evaluara estos resultados.

9.2 Auditoría interna.

Otra de las actividades fundamentales dentro del proceso de retroalimentación y control de todo sistema es la actividad de verificación o chequeo. En este caso, corresponde al proceso de gestión de la auditoría interna. La norma determina que la organización deberá realizar auditorías internas a intervalos planificados para obtener información sobre el funcionamiento del SGSI en relación a:

- a) es conforme con:
 - 1. los requisitos propios de la organización para el SGSI.
 - 2. los requisitos del estándar.
- b) está eficientemente implantado y mantenido. De nuevo se debe valorar el logro de los resultados esperados.

Para ello, se debe planificar, establecer, implementar y mantener un programa de auditoría, incluyendo la frecuencia de las mismas, los métodos, responsabilidades, requisitos de planificación e informes.

De este proceso es esencial asegurar que los resultados se reportan a la dirección, aunque ello se consigue en el proceso de Revisión por Dirección al considerar la auditoría como una de las entradas a dicho proceso.

9.3. Revisión por Dirección.

Como resultado de las actividades de análisis de la gestión (Monitorización, medición y auditoría interna) debe llegar la fase de toma de decisiones o de realización de ajustes.

En todo ciclo de control de sistemas, las desviaciones son gestionadas modificando los criterios de control para lograr que cambien las cosas y que las salidas sean las esperadas. En este proceso de gestión del SGSI, la alta dirección deberá revisar el SGSI a intervalos planificados para asegurar su continua adecuación, vigencia y efectividad.

En este caso, la revisión por la dirección deberá considerar como entradas:

- a. el estado de las acciones de anteriores revisiones.
- b. cambios en asuntos internos o externos que sean relevantes para el SGSI.
- c. retroalimentación del rendimiento de la seguridad de la información, incluyendo estadísticas sobre:
 - no conformidades y acciones correctivas.
 - medición de la monitorización y la medición de resultados
 - resultados de las auditorías,
 - cumplimiento de los objetivos de seguridad.
- c) D) retroalimentación de las partes interesadas.
- d) E) resultados del análisis de riesgos y del estado del plan de tratamiento.
- e) F) oportunidades de mejora continua.

La salida de la revisión de la dirección deberá incluir las decisiones relativas a las oportunidades de mejora continua y las necesidades de cambios del SGSI.

10. Mejora

Esta es el proceso de ajuste o de control de desviaciones del SGSI donde las cosas que no funcionan de forma adecuada son documentadas para aplicar acciones de corrección que mitiguen tanto las consecuencias directas como las causas que las ocasionan.

10.1. No conformidad y acción correctiva.

Este elemento ahora está más claramente descrita y formaliza mejor el proceso de gestión de no conformidades y acciones correctivas indicando como requisitos que cuando una no conformidad se identifique habrá que:

- 1) reaccionar contra la no conformidad y cuando sea aplicable:
 - a. tomar acciones para controlar y corregirla, y
 - b. tratar con sus consecuencias.
- 2) B) evaluar las necesidades de acciones para eliminar las causas de la no conformidad con el objetivo de que no se repita u ocurra de nuevo, mediante:
 - c. revisando la no conformidad.
 - d. determinando las causas de la no conformidad.
 - e. determinando si existen similares no conformidad es o si potencialmente podrían ocurrir.
- 3) C) implementar la acción necesaria.
- 4) D) revisar la efectividad de las acciones correctivas tomadas
- 5) E) hacer cambios en el SGSI si fueran necesarios.

Las acciones correctivas deberán ser adecuadas para los efectos de las no conformidades encontradas.



10.2. Mejora continua

Como filosofía general del ciclo de Deming o PDCA, este elemento determina que el propósito fundamental de la organización deberá ser el mejorar de forma continua la vigencia, adecuación y efectividad del SGSI, es decir, año tras año debe buscarse el consolidar las cosas que se hacen bien, mejorar las que no funcionan o plantearse nuevos controles para seguir reduciendo niveles de riesgo y los umbrales de aceptación de los mismos.