Sistema de Gestión de la Seguridad de la Información

El SGSI (Sistema de Gestión de Seguridad de la Información) es el concepto sobre el que se construye ISO 27001.

La gestión de la seguridad de la información debe realizarse mediante

un proceso sistemático,

documentado

y conocido por toda la organización.

Este proceso es el que constituye un SGSI, que podría considerarse, por analogía con una norma tan conocida como la ISO 9001, como el sistema de calidad para la seguridad de la información.

Garantizar un nivel de protección total es imposible incluso en el caso de disponer de un presupuesto ilimitado

El propósito de un sistema de gestión de la seguridad de la información es,

por tanto, garantizar que los riesgos de la seguridad de la información:

son conocidos,

asumidos,

gestionados

y minimizados

por la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías.

¿**Qué es un SGSI?**

SGSI es la abreviatura comúnmente utilizada para referirse a un Sistema de Gestión de la Seguridad de la Información. ISMS son las siglas equivalentes en el idioma inglés y en relación a *Information Security Management System*.

Por información:

se entiende toda aquella documentación en poder de una organización e independientemente de la forma en que se guarde o transmita (escrita, representada mediante diagramas o impresa en papel, almacenada electrónicamente, proyectada en imágenes, enviada por fax o correo, o, incluso, transmitida de forma oral en una conversación presencial o telefónica), de su origen (de la propia organización o de fuentes externas) y de la fecha de elaboración.

La seguridad de la información consiste en la preservación de su

confidencialidad,

integridad

y disponibilidad,

así como de los sistemas implicados en su tratamiento, dentro de una organización. Así pues, estos tres términos constituyen la base sobre la que se cimienta todo el edificio de la seguridad de la información:

- Confidencialidad: acceso a la información por parte únicamente de quienes estén autorizados.
- Integridad: mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.
- Disponibilidad: Acceso a la información y los sistemas de tratamiento de la misma por parte de los usuarios autorizados cuando lo requieran.

Para garantizar que la seguridad de la información es gestionada correctamente, se debe hacer uso de un proceso sistemático, documentado y conocido por toda la organización. Este proceso es el que constituye un SGSI, que podría considerarse, por analogía con una norma tan conocida como la ISO 9001, como el sistema de calidad de la seguridad de la información.

¿Para qué sirve un SGSI?

La información, junto a los procesos y sistemas que hacen uso de ella, son **activos** muy importantes de una organización. La confidencialidad, integridad y disponibilidad de información sensible pueden llegar a ser esenciales para mantener los niveles de competitividad, rentabilidad, conformidad legal e imagen empresarial necesarios para lograr los objetivos de la organización y asegurar beneficios económicos.

Las organizaciones y sus sistemas de información están expuestos a un número cada vez más elevado de amenazas que pueden aprovechar cualquiera de las vulnerabilidades existentes en la organización para someter activos críticos de información a diversas formas de fraude, espionaje, sabotaje o vandalismo. Los virus informáticos, el "hacking" o los ataques de denegación de servicio son algunos ejemplos comunes y conocidos por su elevado nivel de sofisticación, pero también se deben considerar los riesgos a sufrir incidentes de seguridad causados voluntaria o involuntariamente desde dentro de la propia organización o aquéllos provocados accidentalmente

por catástrofes naturales.

El cumplimiento de la legalidad, la adaptación dinámica y puntual a las condiciones variables del entorno, la protección adecuada de los objetivos de negocio para asegurar el máximo beneficio o el aprovechamiento de nuevas oportunidades de negocio son algunos de los aspectos fundamentales en los que un SGSI significa una herramienta definitiva para su consecución en las organizaciones y de importante ayuda para la gestión de las mismas.

El nivel de seguridad alcanzado por medios técnicos demuestra ser invariablemente limitado e insuficiente por sí mismo. En la gestión efectiva de la seguridad debe tomar parte activa toda la organización con la dirección al frente y se debe considerar, adicionalmente, a clientes y proveedores de bienes y servicios. El modelo de gestión de la seguridad debe contemplar unos procedimientos adecuados y la planificación e implantación de controles de seguridad basadas en una evaluación de riesgos y una medición de la eficacia de los mismos.

El Sistema de Gestión de la Seguridad de la Información (SGSI) ayuda a establecer estas políticas y procedimientos en relación a los objetivos propios y de negocio de la organización, con objeto de mantener un nivel de exposición siempre menor al nivel de riesgo que la propia organización ha decidido asumir.

Con un SGSI, la organización conoce los riesgos a los que está sometida su información y los asume, minimiza, transfiere o controla mediante una sistemática definida, documentada y conocida por todos, que se revisa y actualiza constantemente.

¿Qué incluye un SGSI?

Un Sistema de Gestión de la Seguridad de la Información basado en ISO 27001 está formado por una serie de documentos que pueden clasificarse en una pirámide de cuatro niveles.

La documentación debe incluir los registros de las decisiones de la dirección, asegurar que se puedan seguir los indicios de las decisiones de la dirección y las políticas, así como permitir que los resultados registrados sean reproducibles.

Una demostración clásica que suele solicitarse por los auditores es la realización del camino inverso, es decir, partiendo desde los controles seleccionados se observan los resultados del proceso de evaluación y tratamiento del riesgo hasta alcanzar la política del SGSI y los objetivos iniciales.

La documentación de un SGSI deberá incluir:

Documentos de Nivel 1

Forman el manual de seguridad. Son los siguientes:

- **Alcance del SGSI**: ámbito de la organización que queda sometido al SGSI. Se debe incluir una identificación clara de las dependencias, relaciones y límites que existen entre el alcance y aquellas partes que no hayan sido consideradas, prestando especial atención en aquellos casos en los que el ámbito de influencia del SGSI considere una parte menor de la organización como delegaciones, divisiones, áreas, procesos o tareas concretas.

- **Política y objetivos de seguridad**: documento de contenido genérico que establece el compromiso de la dirección y el enfoque de la organización en la gestión de la seguridad de la información.

- **Metodología de evaluación de riesgos**: descripción de cómo se realizará la evaluación de las amenazas, vulnerabilidades, probabilidades de ocurrencia e impactos en relación a los activos de información contenidos dentro del alcance seleccionado.

- **Informe de evaluación de riesgos**: estudio resultante de aplicar la metodología de evaluación anteriormente mencionada.

- **Plan de tratamiento del riesgo**: documento que define las acciones para reducir, prevenir, transferir o asumir los riesgos de seguridad de la información e implantar los controles necesarios para proteger la misma.

- **Declaración de aplicabilidad** (SOA -Statement of Applicability-, en sus siglas inglesas): documento que contiene los objetivos de control y los controles contemplados por el SGSI, basado en los resultados de los procesos de evaluación y tratamiento de riesgos, justificando inclusiones y exclusiones.

- **Procedimientos relativos al nivel 1**: procedimientos que regulan cómo se realizan,

gestionan y mantienen los documentos enumerados en el nivel 1.

Documentos de Nivel 2

Procedimientos: documentos que aseguran que se realicen de forma eficaz la planificación, operación y control de los procesos de seguridad de la información y describen cómo medir la efectividad de los controles.

Documentos de Nivel 3

Instrucciones, *checklists* y formularios: documentos que describen cómo se realizan las tareas y las actividades específicas relacionadas con la seguridad de la información.

Documentos de Nivel 4.

Registros: documentos que proporcionan una evidencia objetiva del cumplimiento de los requisitos del SGSI; están asociados a documentos de los otros tres niveles como *output* que demuestra que se ha cumplido lo indicado en los mismos.

Control de la documentación.

Para los documentos generados se debe establecer, documentar, implantar y mantener un procedimiento que defina las acciones de gestión necesarias para:

- Aprobar documentos apropiados antes de su emisión.
- Revisar y actualizar documentos cuando sea necesario y renovar su validez.
- Garantizar que los cambios y el estado actual de revisión de los documentos están identificados.
- Garantizar que las versiones relevantes de documentos vigentes están disponibles en los lugares de empleo.
- Garantizar que los documentos se mantienen legibles y fácilmente identificables.
- Garantizar que los documentos permanecen disponibles para aquellas personas que los necesiten y que son transmitidos, almacenados y finalmente desechados acorde con los procedimientos aplicables según su clasificación.
- Garantizar que los documentos procedentes del exterior están identificados.
- Garantizar que la distribución de documentos está controlada.
- Prevenir la utilización de documentos obsoletos
- Aplicar la identificación apropiada de documentos si son retenidos por algún propósito.

¿Cómo se implementa un SGSI?

Para establecer y gestionar un Sistema de Gestión de la Seguridad de la Información en base a ISO 27001, se utiliza el ciclo continuo PDCA, tradicional en los sistemas de gestión de la calidad.

- ***Plan (planificar):*** establecer el SGSI.
- ***Do (hacer):*** implementar y utilizar el SGSI.
- ***Check (verificar):*** monitorizar y revisar el SGSI.
- ***Act (actuar):*** mantener y mejorar el SGSI.

***Plan:* Establecer el SGSI**

- **Definir el alcance** del SGSI en términos del negocio, la organización, su localización, activos y tecnologías, incluyendo detalles y justificación de cualquier exclusión.
- Definir una política de seguridad que:

– incluya el marco general y los objetivos de seguridad de la información de la organización;

– considere requerimientos legales o contractuales relativos a la seguridad de la información;

– esté alineada con el contexto estratégico de gestión de riesgos de la organización en el que se establecerá y mantendrá el SGSI;

– establezca los criterios con los que se va a evaluar el riesgo;

– esté aprobada por la dirección.

• Definir una metodología de evaluación del riesgo apropiada para el SGSI y los requerimientos del negocio que especifique los niveles de riesgo aceptables y unos criterios de aceptación de los riesgos. Lo primordial de esta metodología es que los resultados obtenidos sean comparables y reproducibles. (Existen distintas metodologías para la evaluación de riesgos y se pueden encontrar algunos ejemplos en la guía para la gestión de la seguridad ISO 13335-3.)

• **Identificar los riesgos:**

– identificar los activos que están dentro del alcance del SGSI y a sus responsables directos, denominados propietarios;

– Identificar las amenazas en relación a los activos;

– Identificar las vulnerabilidades que puedan ser aprovechadas por dichas amenazas;

– Identificar los impactos en la confidencialidad, integridad y disponibilidad de los activos.

• **Analizar y evaluar los riesgos:**

– evaluar el impacto en el negocio de la organización de un fallo de seguridad que suponga la pérdida de confidencialidad, integridad o disponibilidad de un activo de información;

– evaluar de forma realista la probabilidad de ocurrencia de un fallo de seguridad en relación a las amenazas, vulnerabilidades, impactos en los activos y los controles que ya estén implementados;

– estimar los niveles de riesgo;

– determinar, según los criterios de aceptación de riesgo previamente establecidos, si el riesgo es aceptable o necesita ser tratado.

• **Identificar y evaluar** las distintas opciones de tratamiento de los riesgos para:

– aplicar controles adecuados;

– aceptar el riesgo, siempre y cuando se siga cumpliendo con las políticas y criterios establecidos para la aceptación de los riesgos;

– evitar el riesgo, por ej. mediante el cese de las actividades que lo originan;

– transferir el riesgosa terceros, por ej. aseguradoras o proveedores.

• **Seleccionar los objetivos de control y los controles** del Anexo A de la norma ISO 27001 para el tratamiento del riesgo y que cumplan con los requerimientos identificados en el proceso de evaluación y tratamiento del riesgo.

• **Aprobar por parte de la dirección tanto los riesgos residuales** como la implantación y uso del SGSI.

• **Definir una declaración de aplicabilidad que incluya**:

– los objetivos de control y controles seleccionados y los motivos para su elección;

– los objetivos de control y controles que actualmente ya están implantados;

– los objetivos de control y controles del Anexo A excluidos y los motivos para su exclusión. Este es un mecanismo que permite, además, detectar posibles omisiones involuntarias.

En relación a los controles de seguridad, el estándar ISO/IEC 17799 proporciona una completa guía de implantación que contiene 133 controles, según 39 objetivos de control agrupados en 11 cláusulas.

El estándar ISO 27001 referencia en su segunda cláusula a la guía ISO/IEC 17799 en términos de "documento indispensable para la aplicación de este documento" y deja abierta la posibilidad de incluir controles adicionales en el caso que la guía no contemplase ciertas necesidades particulares.

Do: Implementar y utilizar el SGSI

- Definir un plan de tratamiento de riesgos que identifique las acciones, recursos, responsabilidades y prioridades en la gestión de los riesgos de seguridad de la información.
- Implantar el plan de tratamiento de riesgos, con el fin de alcanzar los objetivos de control identificados y que incluya la financiación, la asignación de roles y responsabilidades.
- Implementar los controles anteriormente seleccionados que lleven a los objetivos de control.
- Definir un sistema de métricas que permita obtener resultados reproducibles y comparables para medir la eficacia de los controles seleccionados.
- Procurar programas de formación y concienciación en relación a la seguridad de la información dirigidos a todo el personal.
- Gestionar las operaciones del SGSI.
- Gestionar los recursos necesarios asignados al SGSI para el mantenimiento de la seguridad de la información.
- Implantar procedimientos y controles que permitan una rápida detección y respuesta a los incidentes de seguridad.

Check: Monitorizar y revisar el SGSI

La organización deberá:

- Ejecutar procedimientos de monitorización y revisión para:

– la detección temprana de errores en los resultados generados por los procesos;

– la identificación temprana de brechas e incidentes de seguridad;

– capacitar a la dirección para determinar si las actividades desarrolladas por las personas y dispositivos tecnológicos para garantizar la seguridad de la información se desarrollan en relación a lo previsto;

– detectar y prevenir eventos e incidentes de seguridad mediante el uso de indicadores;

– determinar si las acciones realizadas para resolver brechas de seguridad fueron efectivas.

- Revisar regularmente la efectividad del SGSI, atendiendo al cumplimiento de la política y objetivos del SGSI, los resultados de auditorías de seguridad, incidentes, resultados de las mediciones de eficacia, sugerencias y observaciones de todas las partes implicadas.
- Medir la efectividad de los controles para verificar que se cumple con los requisitos de seguridad.
- Revisar regularmente en intervalos planificados las evaluaciones de riesgo, los riesgos residuales y sus niveles aceptables, teniendo en cuenta los posibles cambios que hayan podido producirse en la organización, la tecnología, los objetivos y procesos de negocio, las amenazas identificadas, la efectividad de los controles implementados y el entorno exterior -requerimientos

legales, obligaciones contractuales, etc.-.

- Realizar periódicamente auditorías internas del SGSI en intervalos planificados.
- Revisar el SGSI por parte de la dirección periódicamente para garantizar que el alcance definido sigue siendo el adecuado y que las mejoras en el proceso del SGSI son evidentes.
- Actualizar los planes de seguridad en función de las conclusiones y nuevos hallazgos encontrados durante las actividades de monitorización y revisión.
- Registrar acciones y eventos que puedan haber impactado sobre la efectividad o el rendimiento del SGSI.

Act: Mantener y mejorar el SGSI

La organización deberá regularmente:

- Implantar en el SGSI las mejoras identificadas.
- Realizar las acciones preventivas y correctivas adecuadas en relación a la claúsula 8 de la norma ISO 27001 y a las lecciones aprendidas de las experiencias propias y de otras organizaciones.
- Comunicar las acciones y mejoras a todas las partes interesadas con el nivel de detalle adecuado y acordar, si es pertinente, la forma de proceder.
- Asegurarse que las mejoras introducidas alcanzan los objetivos previstos.

PDCA es un ciclo de vida continuo, lo cual quiere decir que la fase de *Act* lleva de nuevo a la fase de *Plan* para iniciar un nuevo ciclo de las cuatro fases.

¿Qué tareas tiene la Gerencia en un SGSI?

Uno de los componentes primordiales en la implantación exitosa de un sistema de gestión de seguridad de la información **es la implicación de la dirección**. No se trata de una expresión retórica, sino que debe asumirse desde un principio que un SGSI afecta fundamentalmente a la gestión del negocio y requiere, por tanto, de decisiones y acciones que sólo puede tomar la gerencia de la organización. No se debe caer en el error de considerar un SGSI una mera cuestión técnica relegada a niveles inferiores del organigrama; se están gestionando riesgos e impactos de negocio que son responsabilidad y decisión de la dirección.

El término Dirección debe contemplarse siempre desde el punto de vista del alcance del SGSI. Es decir, se refiere al nivel más alto de gerencia de la parte de la organización afectada por el SGSI (recuérdese que el alcance no tiene por qué ser toda la organización).

Algunas de las tareas fundamentales del SGSI que ISO 27001 asigna a la dirección se detallan en los siguientes puntos.

Compromiso de la dirección

La dirección de la organización debe comprometerse con el establecimiento, implementación, operación, monitorización, revisión, mantenimiento y mejora del SGSI. Para ello, debe tomar las siguientes iniciativas:

- Establecer una política de seguridad de la información.
- Asegurarse de que se establecen objetivos y planes del SGSI.
- Establecer roles y responsabilidades de seguridad de la información.
- Comunicar a la organización tanto la importancia de lograr los objetivos de seguridad de la información y de cumplir con la política de seguridad, como sus responsabilidades legales y la necesidad de mejora continua.

- Asignar suficientes recursos al SGSI en todas sus fases.
- Decidir los criterios de aceptación de riesgos y sus correspondientes niveles.
- Asegurar que se realizan auditorías internas.
- Realizar revisiones del SGSI, como se detalla más adelante.

Asignación de recursos

Para el correcto desarrollo de todas las actividades relacionadas con el SGSI, es imprescindible la asignación de recursos. Es responsabilidad de la dirección garantizar que se asignan los suficientes para:

- Establecer, implementar, operar, monitorizar, revisar, mantener y mejorar el SGSI.
- Garantizar que los procedimientos de seguridad de la información apoyan los requerimientos de negocio.
- Identificar y tratar todos los requerimientos legales y normativos, así como las obligaciones contractuales de seguridad.
- Aplicar correctamente todos los controles implementados, manteniendo de esa forma la seguridad adecuada.
- Realizar revisiones cuando sea necesario y actuar adecuadamente según los resultados de las mismas.
- Mejorar la eficacia del SGSI donde sea necesario.

Formación y concienciación

La formación y la concienciación en seguridad de la información son elementos básicos para el éxito de un SGSI. Por ello, la dirección debe asegurar que todo el personal de la organización al que se le asignen responsabilidades definidas en el SGSI esté suficientemente capacitado y se

- determinen las competencias necesarias para el personal que realiza tareas en aplicación del SGSI,
- satisfagan dichas necesidades por medio de formación o de otras acciones como, p. ej., contratación de personal ya formado,
- evalúe la eficacia de las acciones realizadas,
- mantengan registros de estudios, formación, habilidades, experiencia y cualificación.

Además, la dirección debe asegurar que todo el personal relevante está concienciado de la importancia de sus actividades de seguridad de la información y de cómo contribuye a la consecución de los objetivos del SGSI.

Revisión del SGSI

A la dirección de la organización se le asigna también la tarea de, al menos una vez al año, revisar el SGSI, para asegurar que continúe siendo adecuado y eficaz. Para ello, debe recibir una serie de informaciones, que le ayuden a tomar decisiones, entre las que se pueden enumerar:

- Resultados de auditorías y revisiones del SGSI.
- Observaciones de todas las partes interesadas.
- Técnicas, productos o procedimientos que pudieran ser útiles para mejorar el rendimiento y eficacia del SGSI.
- Información sobre el estado de acciones preventivas y correctivas.
- Vulnerabilidades o amenazas que no fueran tratadas adecuadamente en evaluaciones de riesgos anteriores.

- Resultados de las mediciones de efectividad.
- Estado de las acciones iniciadas a raíz de revisiones anteriores de la dirección.
- Cualquier cambio que pueda afectar al SGSI.
- Recomendaciones de mejora.

Basándose en todas estas informaciones, la dirección debe revisar el SGSI y tomar decisiones y acciones relativas a:

- Mejora de la eficacia del SGSI.
- Actualización de la evaluación de riesgos y del plan de tratamiento de riesgos.
- Modificación de los procedimientos y controles que afecten a la seguridad de la información, en respuesta a cambios internos o externos en los requerimientos de negocio, requerimientos de seguridad, procesos de negocio, marco legal, obligaciones contractuales, niveles de riesgo y criterios de aceptación de riesgos.
- Necesidades de recursos.
- Mejora de la forma de medir la efectividad de los controles.

¿Se integra un SGSI con otros sistemas de gestión?

Un SGSI es, en primera instancia, un sistema de gestión, es decir, una herramienta de la que dispone la gerencia para dirigir y controlar un determinado ámbito, en este caso, la seguridad de la información.

La gestión de las actividades de las organizaciones se realiza, cada vez con más frecuencia, según sistemas de gestión basados en estándares internacionales:

se gestiona la calidad según ISO 9001,

el impacto medioambiental según ISO 14001

o la prevención de riesgos laborales según OHSAS 18001.

Ahora, añadimos ISO 27001 como estándar de gestión de seguridad de la información.

Las empresas tienen la posibilidad de implantar un número variable de estos sistemas de gestión para mejorar la organización y beneficios sin imponer una carga a la organización.

El objetivo último es llegar a un único sistema de gestión que contemple todos los aspectos necesarios para la organización, basándose en el ciclo PDCA y el proceso de mejora continua comunes a todos estos estándares. Las facilidades para la integración de las normas ISO son evidentes mediante la consulta de sus anexos.

ISO 27001 detalla en su Anexo C, punto por punto, la correspondencia entre esta norma y la ISO 9001 e ISO 14001. Ahí se observa la alta correlación existente y se puede intuir la posibilidad de integrar el sistema de gestión de seguridad de la información en los sistemas de gestión existentes ya en la organización. Algunos puntos que suponen una novedad en ISO 27001 frente a otros estándares son la evaluación de riesgos y el establecimiento de una declaración de aplicabilidad (SOA), aunque ya se estudia incorporar éstos al resto de normas en un futuro próximo.

En nuestras secciones de Faqs y de Artículos, podrá encontrar más informaciones acerca de la integración del SGSI con otros sistemas de gestión.

Certificación

La norma ISO 27001, al igual que su antecesora BS 7799-2, es certificable. Esto quiere decir que la organización que tenga implantado un SGSI puede solicitar una auditoría a una entidad

certificadora acreditada y, caso de superar la misma con éxito, obtener una certificación del sistema según ISO 27001.

En las siguientes secciones, se abordan diferentes temas relacionados con la certificación.

Acceda directamente a cada una de ellas desde el menú del recuadro verde de la izquierda o descargue en pdf el documento completo.

Implantación del SGSI

Evidentemente, el paso previo a intentar la certificación es la implantación en la organización del sistema de gestión de seguridad de la información según ISO 27001. Este sistema deberá tener un historial de funcionamiento demostrable de al menos tres meses antes de solicitar el proceso formal de auditoría para su primera certificación.

ISO 27001 exige que el SGSI contemple los siguientes puntos:

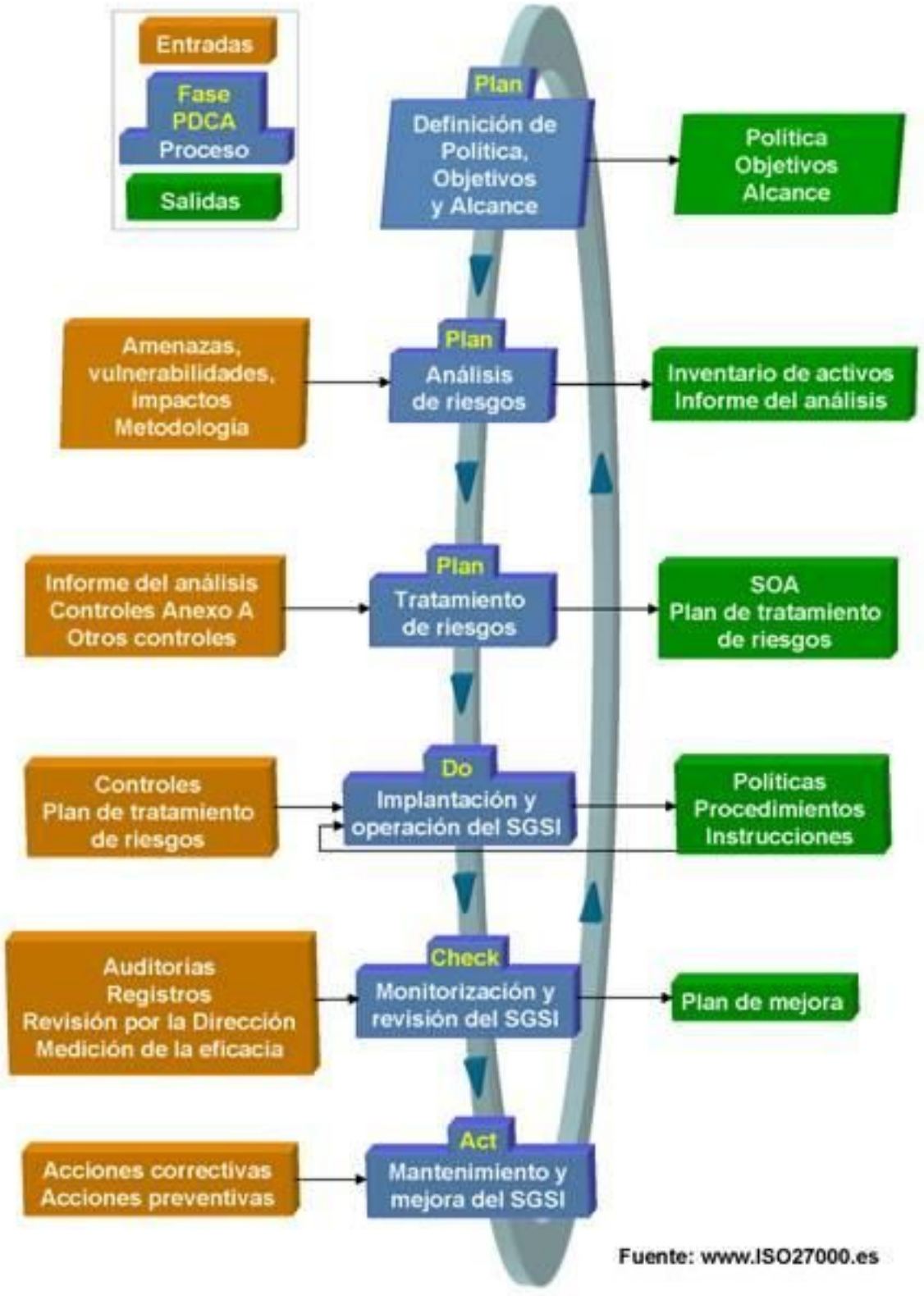
- Implicación de la Dirección.
- Alcance del SGSI y política de seguridad.
- Inventario de todos los activos de información.
- Metodología de evaluación del riesgo.
- Identificación de amenazas, vulnerabilidades e impactos.
- Análisis y evaluación de riesgos.
- Selección de controles para el tratamiento de riesgos.
- Aprobación por parte de la dirección del riesgo residual.
- Declaración de aplicabilidad.
- Plan de tratamiento de riesgos.
- Implementación de controles, documentación de políticas, procedimientos e instrucciones de trabajo.
- Definición de un método de medida de la eficacia de los controles y puesta en marcha del mismo.
- Formación y concienciación en lo relativo a seguridad de la información a todo el personal.
- Monitorización constante y registro de todas las incidencias.
- Realización de auditorías internas.
- Evaluación de riesgos periódica, revisión del nivel de riesgo residual, del propio SGSI y de su alcance.
- Mejora continua del SGSI.

La documentación del SGSI deberá incluir:

- Política y objetivos de seguridad.
- Alcance del SGSI.
- Procedimientos y controles que apoyan el SGSI.
- Descripción de la metodología de evaluación del riesgo.
- Informe resultante de la evaluación del riesgo.
- Plan de tratamiento de riesgos.
- Procedimientos de planificación, manejo y control de los procesos de seguridad de la

información y de medición de la eficacia de los controles.

- Registros.
- Declaración de aplicabilidad (SOA -Statement of Applicability-).
- Procedimiento de gestión de toda la documentación del SGSI.



Hay una serie de controles clave que un auditor va a examinar siempre en profundidad:

- Política de seguridad.
- Asignación de responsabilidades de seguridad.
- Formación y capacitación para la seguridad.
- Registro de incidencias de seguridad.
- Gestión de continuidad del negocio.
- Protección de datos personales.
- Salvaguarda de registros de la organización.
- Derechos de propiedad intelectual.

El SGSI puede estar integrado con otro tipo de sistemas (ISO 9001, ISO 14001…). La propia norma ISO 27001 incluye en su anexo C una tabla de correspondencias de ISO 27001:2005 con ISO 9001:2000 e ISO 14001:2004 y sus semejanzas en la documentación necesaria, con objeto de facilitar la integración.

Es recomendable integrar los diferentes sistemas, en la medida que sea posible y práctico. En el caso ideal, es posible llegar a un solo sistema de gestión y control de la actividad de la organización, que se puede auditar en cada momento desde la perspectiva de la seguridad de la información, la calidad, el medio ambiente o cualquier otra.

Auditoría y certificación

Una vez implantado el SGSI en la organización, y con un historial demostrable de al menos 3 meses, se puede pasar a la fase de auditoría y certificación, que se desarrolla de la siguiente forma:

- Solicitud de la auditoría por parte del interesado a la entidad de certificación y toma de datos por parte de la misma.
- Respuesta en forma de oferta por parte de la entidad certificadora.
- Compromiso.
- Designación de auditores, determinación de fechas y establecimiento conjunto del plan de auditoría.
- Pre-auditoría: opcionalmente, puede realizarse una auditoría previa que aporte información sobre la situación actual y oriente mejor sobre las posibilidades de superar la auditoría real.
- Fase 1 de la auditoría: no necesariamente tiene que ser in situ, puesto que se trata del análisis de la documentación por parte del Auditor Jefe y la preparación del informe de la documentación básica del SGSI del cliente, destacando los posibles incumplimientos de la norma que se verificarán en la Fase 2. Este informe se envía junto al plan de auditoría al cliente. El periodo máximo entre la Fase 1 y Fase 2 es de 6 meses.
- Fase 2 de la auditoría: es la fase de detalle de la auditoría, en la que se revisan in situ las políticas, la implantación de los controles de seguridad y la eficacia del sistema en su conjunto. Se inicia con una reunión de apertura donde se revisa el objeto, alcance, el proceso, el personal, instalaciones y recursos necesarios, así como posibles cambios de última hora. Se realiza una revisión de las exclusiones según la Declaración de Aplicabilidad (documento SOA), de los hallazgos de la Fase 1, de la implantación de políticas, procedimientos y controles y de todos aquellos puntos que el auditor considere de interés. Finaliza con una reunión de cierre en la que se presenta el informe de auditoría.
- Certificación: en el caso de que se descubran durante la auditoría no conformidades graves, la organización deberá implantar acciones correctivas; una vez verificada dicha implantación o, directamente, en el caso de no haberse presentado no conformidades, el auditor podrá emitir un

informe favorable y el SGSI de organización será certificado según ISO 270001.

- Auditoría de seguimiento: semestral o, al menos, anualmente, debe realizarse una auditoría de mantenimiento; esta auditoría se centra, generalmente, en partes del sistema, dada su menor duración, y tiene como objetivo comprobar el uso del SGSI y fomentar y verificar la mejora continua.
- Auditoría de re-certificación: cada tres años, es necesario superar una auditoría de certificación formal completa como la descrita.

Las organizaciones certificadas a nivel mundial en ISO 27001 (o, anteriormente, en BS 7799-2) por entidades acreditadas figuran listadas en http://www.iso27001certificates.com. Para aquellas organizaciones que lo han autorizado, también está publicado el alcance de certificación.

Naturalmente, la organización que implanta un SGSI no tiene la obligación de certificarlo. Sin embargo, sí es recomendable ponerse como objetivo la certificación, porque supone la oportunidad de recibir la confirmación por parte de un experto ajeno a la empresa de que se está gestionando correctamente la seguridad de la información, añade un factor de tensión y de concentración en una meta a todos los miembros del proyecto y de la organización en general y envía una señal al mercado de que la empresa en cuestión es confiable y es gestionada transparentemente.

La entidad de certificación

Las entidades de certificación son organismos de evaluación de la conformidad, encargados de evaluar y realizar una declaración objetiva de que los servicios y productos cumplen unos requisitos específicos. En el caso de ISO 27001, certifican, mediante la auditoría, que el SGSI de una organización se ha diseñado, implementado, verificado y mejorado conforme a lo detallado en la norma.

Existen numerosas entidades de certificación en cada país, ya que se trata de una actividad empresarial privada con un gran auge en el último par de décadas, debido a la creciente estandarización y homologación de productos y sistemas en todo el mundo. La organización que desee certificarse puede contactar a diversas entidades certificadoras y solicitar presupuesto por los servicios ofrecidos, comparando y decidiéndose por la más conveniente, como hace con cualquier otro producto o servicio.

Para que las entidades de certificación puedan emitir certificados reconocidos, han de estar acreditadas. Esto quiere decir que un tercero, llamado organismo de acreditación, comprueba, mediante evaluaciones independientes e imparciales, la competencia de las entidades de certificación para la actividad objeto de acreditación. En cada país suele haber una sola entidad de acreditación (en algunos, hay más de una), a la que la Administración encarga esa tarea. En España, es ENAC (Entidad Nacional de Acreditación); para otros países, puede consultarse una lista.

La acreditación de entidades de certificación para ISO 27001 o para BS 7799-2 -antes de derogarse- suele hacerse en base al documento EA 7/03 "Directrices para la acreditación de organismos operando programas de certificación/registro de sistemas de gestión de seguridad en la información". En el futuro, será la norma ISO 27006 la que regule directamente estas cuestiones.

Las entidades de acreditación establecen acuerdos internacionales para facilitar el reconocimiento mutuo de acreditaciones y el establecimiento de criterios comunes. Para ello, existen diversas asociaciones como IAF (International Accreditation Forum) o EA (European co-operation for Accreditation).

El auditor

El auditor es la persona que comprueba que el SGSI de una organización se ha diseñado, implementado, verificado y mejorado conforme a lo detallado en la norma. En general, se

distinguen tres clases de auditores:

- de primera parte: auditor interno que audita la organización en nombre de sí misma, normalmente, como mantenimiento del sistema de gestión y como preparación a la auditoría de certificación;
- de segunda parte: auditor de cliente, es decir, que audita una organización en nombre de un cliente de la misma; por ejemplo, una empresa que audita a su proveedor de outsourcing;
- de tercera parte: auditor independiente, que audita una organización como tercera parte imparcial; normalmente, porque la organización tiene la intención de lograr la certificación y contrata para ello los servicios de una entidad de certificación.

El auditor, sobre todo si actúa como de tercera parte, ha de disponer también de una certificación personal. Esto quiere decir que, nuevamente un tercero, certifica que posee las competencias profesionales y personales necesarias para desempeñar la labor de auditoría de la materia para la que está certificado.

En este punto, hay pequeñas diferencias entre las entidades certificadoras, que pueden formular requisitos distintos para homologar a sus auditores. Pero, en general, la certificación de auditores se ciñe a la norma ISO 19011 de directrices para la auditoría de sistemas de gestión, que dedica su punto 7 a la competencia y evaluación de los auditores. Al auditor se le exigen una serie de atributos personales, conocimientos y habilidades, educación formal, experiencia laboral y formación como auditor.

Existen diversas organizaciones internacionales de certificación de auditores, con el objeto de facilitar la estandarización de requerimientos y garantizar un alto nivel de profesionalidad de los auditores, además de homologar a las instituciones que ofrecen cursos de formación de auditor. Algunas de estas organizaciones son IRCA, RABQSA o IATCA.

IRCA (International Register of Certificated Auditors) es el mayor organismo mundial de certificación de auditores de sistemas de gestión. Tiene su sede en el Reino Unido y, por ello -debido al origen inglés de la norma BS 7799-2 y, por tanto, de ISO 27001-, tiene ya desde hace años un programa de certificación de auditores de sistemas de gestión de seguridad de la información. Su página web, también en español, es una buena fuente de consulta de los requisitos y los grados de auditor. Dispone de un enlace directo a las últimas novedades del IRCA desde nuestra sección de boletines.

En cuanto a la práctica de la auditoría, al auditor se le exige que se muestre ético, con mentalidad abierta, diplomático, observador, perceptivo, versátil, tenaz, decidido y seguro de sí mismo. Estas actitudes son las que deberían crear un clima de confianza y colaboración entre auditor y auditado. El auditado debe tomar el proceso de auditoría siempre desde un punto de vista constructivo y de mejora continua, y no de fiscalización de sus actividades. Para ello, el auditor debe fomentar en todo momento un ambiente de tranquilidad, colaboración, información y trabajo conjunto.