COLEGIO OFICIAL DE INGENIEROS DE TELECOMUNICACIÓN

Guía de Iniciación a Actividad Profesional Implantación de Sistemas de Gestión de la Seguridad de la Información (*SGSI*) según la norma ISO 27001

colegio oficial
ingenieros de telecomunicación

GRUPO DE NUEVAS ACTIVIDADES PROFESIONALES

Grupo de Nuevas Actividades Profesionales del COIT (Grupo NAP)

En acuerdo de Junta de Gobierno del COIT desde julio de 2009, el Grupo de trabajo de "Nuevas Actividades Profesionales" (NAP), se enmarca dentro del Grupo de trabajo de Ejercicio Profesional, que queda conformado por los Grupos NAP y ELP (Ejercicio Libre Profesional).

Este Grupo de Trabajo nació en el 2003 con el objetivo de ocuparse de detectar nuevas actividades que surjan, analizarlas, evaluar su impacto y, en su caso, promocionarlas. Una resultante de esta misión es promover, en su caso, la conveniencia o la obligatoriedad de contar con la redacción de un proyecto técnico de telecomunicaciones en estas nuevas áreas de actividad, ya sea por su grado de complejidad, porque soporten servicios de telecomunicación de uso público, porque deban quedar garantizados unos requisitos mínimos de calidad y de seguridad o bien porque se deba hacer un uso eficaz y eficiente de ciertos recursos públicos limitados en un régimen de mercado liberalizado.

Este documento se enmarca dentro de una nueva serie de estudios breves denominados "Guías de Iniciación a Actividades Profesionales" que pretenden dar respuesta a todas aquellas cuestiones que puedan plantearse de manera práctica y didáctica a aquellos que quieran adentrarse en nuevas actividades profesionales.

Esperamos que sea de vuestro de interés

Cayetano Lluch Mesquida

Vicedecano del COIT

Agradecimientos

En la redacción de esta guía se ha contado con la valiosa ayuda y experiencia de nuestro compañero Jesús Sánchez López al que agradecemos desde estas líneas su dedicación y esfuerzo.

ÍNDICE

ÍNDICE DE FIGURAS

1. INTRODUCCIÓN

La disciplina denominada tradicionalmente "Seguridad Informática" ha evolucionado a una velocidad vertiginosa en la breve (no más allá de 60 años) pero intensa historia de los ordenadores y de la Informática.

El objetivo inicial de proteger, frente a causas accidentales o intencionadas, los costosos equipos de Proceso de Datos de los años [19]50-60 ha quedado, por distintos motivos, obsoleto. La prioridad actual es proteger la Información como activo vital para cualquier Organización y hacerlo en diferentes dimensiones: ***D***isponibilidad, ***I***ntegridad, ***C***onfidencialidad y ***A***utenticidad (***ACID***).

En consecuencia, se hace necesario evolucionar hacia el concepto de **Sistema de Gestión de la Seguridad de la Información** (**SGSI**- ***ISMS =I****nformation* ***S****ecurity* ***M****anagement* ***S****ystem)* que se ocupe no solo de la problemática (debilidades, amenazas, incidencias, etc.) de la componente tecnológica (**seguridad TIC**) sino que lo haga desde un enfoque global abordando, además, otros aspectos: normativos, legales, organizativos e incluso (y sobre todo) culturales y cuyo planteamiento se conciba desde la visión de ***problema de negocio***. Definimos el Sistema de Gestión de la Seguridad de la Información (ISO 27001:2005) como:

> *La parte del sistema de gestión general, basada en un enfoque de riesgo empresarial, que se establece para crear, implementar, operar, supervisar, revisar, mantener y mejorar la seguridad de la información.*

No es sencillo identificar un claro y único origen del nacimiento de una doctrina en Seguridad de la Información (tal vez no exista) aunque nos parece especialmente reseñable el documento *DIRECTRICES DE LA OCDE PARA LA SEGURIDAD DE SISTEMAS Y REDES DE INFORMACIÓN: HACIA UNA CULTURA DE SEGURIDAD*, publicado en julio de 2002, en cuyo capítulo I puede leerse:

> Estas Directrices pretenden dar respuesta a un ambiente de seguridad cada vez más cambiante, a través de la promoción del desarrollo de una cultura de seguridad – esto es, centrándose en la seguridad del desarrollo de sistemas y redes de información, así como en la adopción de nuevas formas de pensamiento y comportamiento en el uso e interconexión de sistemas y redes de información. Estas Directrices marcan una clara ruptura con un tiempo en el que los aspectos de seguridad y el uso de redes y sistemas se consideraban con frecuencia como elementos a posteriori. Los sistemas, redes y servicios de información afines, deben ser fiables y seguros, dado que los participantes son cada vez más dependientes de éstos. Sólo un enfoque que tome en cuenta los intereses de todos los participantes y la naturaleza de los sistemas, redes y servicios afines puede proporcionar una seguridad efectiva.

Tomando en consideración estas recomendaciones, así como un conjunto de

normas existentes con anterioridad (muy en particular las elaboradas por la *British Standard Institution* –BSI-), la *International Organization for Standardization* (ISO) publicó, en 2005, la norma ISO 27001 a la que siguieron otro conjunto de ellas que se conocen colectivamente como familia ISO 2700x.

Esta norma es aplicable a todo tipo de Organizaciones y sectores de actividad, incluidas las Administraciones Públicas. Existen países (por ejemplo Perú) que las han hecho de obligado cumplimiento en tanto que otros han desarrollado una normativa específica. Tal es el caso de España que lo regula mediante el RD 3/2010 por el que establece el Esquema Nacional de Seguridad como consecuencia de lo dispuesto en la Ley 11/2007 de Acceso Electrónico de los Ciudadanos a los Servicios Públicos.

El SGSI puede integrarse con relativa facilidad con otros Sistemas de Gestión genéricos: Sistema de Gestión de la Calidad (ISO 9001) y el Sistema de Gestión Medioambiental (ISO 14001), Continuidad de Negocio (ISO 22301 y BS 25999), etc., específicos de TI: ISO 20000, ITIL, COBIT, etc., así como otros tipos de marcos regulatorios, en particular el relativo a Protección de Datos de Carácter Personal (LOPD) en un Sistema de Gestión Global que utilice recursos comunes.

La adecuación de las Organizaciones a este tipo de normativas es una actividad emergente (tanto en las vertientes de consultoría como de auditoría) que ofrece a los Ingenieros de Telecomunicación un interesante abanico de posibilidades profesionales tanto específicas del sector TIC como multidisciplinares (Dirección de Proyectos).

No existe (ni se espera) una regulación gubernamental de naturaleza facultativa para el ejercicio de tales actividades por lo que se presenta a nuestro colectivo una interesante oportunidad para alcanzar prestigio y presencia en el sector.

2. LA FAMILIA DE NORMAS ISO 27000.

La serie ISO 27000 contempla un conjunto de estándares desarrollados por ISO e IEC (*International Electrotechnical Commission*), que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización. Las más conocidas son. (Fuente: http:/www.iso27000.es):

- ISO/IEC 27000. Proporciona una visión general de las normas que componen la serie 27000, una introducción a los Sistemas de Gestión de Seguridad de la Información, una breve descripción del proceso *Plan-Do-Check-Act* y términos y definiciones que se emplean en toda la serie 27000.
- ISO/IEC 27001. Es la norma principal de la serie y contiene los requisitos del sistema de gestión de seguridad de la información. Tiene su origen en la BS 7799-2:2002 y es la norma con arreglo a la cual se certifican los SGSI's de las organizaciones. En su Anexo A enumera en forma de resumen los objetivos de control y controles que desarrolla la ISO 27002:2005, para que sean seleccionados por las organizaciones en el desarrollo de sus SGSI.
- ISO/IEC 27002. (Antigua ISO 17799:2005). Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. No es certificable. Contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios.

La tabla siguiente muestra un resumen de la familia:

Norma	Contenido
27000	Visión general de la serie.
27001	Norma principal de la serie. Requisitos del SGSI. Certificable.
27002	Guía de buenas prácticas: (11) dominios, (39) objetivos de control y (133) controles.
27003	Aspectos críticos para el diseño e implementación de un SGSI.
27004	Guía para el desarrollo y utilización de métricas y técnicas de medida de la eficacia de un SGSI y de los controles o grupos de controles.
27005	Directrices para la gestión del riesgo.
27006	Requisitos para la acreditación de entidades de auditoría y certificación.
27007	Guía de auditoría de un SGSI.
27008	Guía de auditoría de los controles seleccionados.
27013	Guía de implementación integrada de ISO/IEC 27001 e ISO/IEC 20000-1.
27014	Guía de gobierno corporativo de la seguridad de la información.
27031	Guía de continuidad de negocio en cuanto a tecnologías de la información y comunicaciones.
27032	Guía relativa a la ciberseguridad.
27033	Guía de seguridad en redes (7 partes).

27034	Guía de seguridad en aplicaciones informáticas.
27035	Guía de gestión de incidentes de seguridad de la información.
27036	Guía de seguridad de externalización de servicios.
27037	Guía de identificación, recopilación y preservación de evidencias digitales

Adicionalmente a las normas anteriores, cuyo ámbito de aplicación es independiente del tipo de actividad desarrollado por la organización, se han elaborado (o están en fase de ello) otras aplicables a sectores específicos:

- ISO/IEC 27010. Es una norma, dividida en dos partes, para la gestión de la seguridad de la información en comunicaciones intersectoriales.
- ISO/IEC 27011 Es una guía de interpretación de la implementación y gestión de la seguridad de la información en organizaciones del sector de telecomunicaciones basada en ISO/IEC 27002. Está publicada también como norma ITU-T X.1051.
- ISO/IEC 27012. Es un conjunto de requisitos (complementarios a ISO/IEC 27001) y directrices (complementarias a ISO/IEC 27002) de gestión de seguridad de la información en organizaciones que proporcionen servicios de e-Administración.
- ISO/IEC 27015. Guía de SGSI para organizaciones del sector financiero y de seguros.
- ISO 27799. Es una norma que proporciona directrices para apoyar la interpretación y aplicación en el sector sanitario de ISO/IEC 27002, en cuanto a la seguridad de la información sobre los datos de salud de los pacientes. Esta norma, al contrario que las anteriores, no la desarrolla el subcomité JTC1/SC27, sino el comité técnico TC 215.

Con diferente finalidad se tiene la Norma ISO 19011 que proporciona orientación relativa a las auditorías de sistemas de gestión. Es de ámbito general y, en consecuencia, aplicable tanto a la Seguridad de la Información (27001) como a la calidad (9001) y a la gestión ambiental (14001).

3. PRESENTACIÓN DE UN SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN SEGÚN LA NORMA ISO 27001.

La norma ISO 27001 es la principal de la serie. En ella se define el concepto de Sistema de Gestión de la Seguridad de la Información, se establece el marco de referencia y se desarrolla la propia norma que, como ya se ha indicado, es certificable. La norma es aplicable a todo tipo de organizaciones o de partes de ellas e incluye la estructura organizativa, las políticas, las actividades de planificación, las responsabilidades, las prácticas, los procedimientos, los procesos y los recursos. Su título completo es:

> Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información (SGSI). Requisitos.

Esta norma internacional, enmarcada dentro de la gestión de riesgos empresariales generales, especifica los requisitos para el establecimiento de controles de seguridad adecuados y proporcionados, que protejan los activos de información y den garantías a las partes interesadas. Algunos de los controles pueden ser excluidos, pero siempre que se justifique que los riesgos asociados han sido aceptados por las personas responsables.

Para la aplicación de la norma es necesario utilizar la norma ISO/IEC 27002: *Código de buenas prácticas para la gestión de la seguridad de la información*.

3.1. Términos y definiciones.

La norma hace uso de las siguientes definiciones[1] :

Aceptación del riesgo.	La decisión de aceptar un riesgo.
Activo.	Cualquier bien que tiene valor para la organización.
Análisis de riesgos.	Utilización sistemática de la información disponible para identificar peligros y estimar los riesgos.
Confidencialidad.	La propiedad por la que la información no se pone a disposición o se revela a individuos, entidades o procesos no autorizados.
Declaración de aplicablidad ***S**tatement **O**f **A**pplicability (**SOA**)*	Declaración documentada que describe los objetivos de control y los controles que son relevantes para el SGSI de la organización y aplicables al mismo.
Disponibilidad.	La propiedad de ser accesible y utilizable por una entidad autorizada.
Estimación de riesgos	El proceso de comparación del riesgo estimado con los criterios de riesgo, para así determinar la importancia del riesgo.
Evaluación de riesgos.	El proceso general de análisis y estimación de riesgos.
Evento de seguridad de la información.	La ocurrencia detectada en un estado de un sistema, servicio o red que indica una posible violación de la política de seguridad de la información, un fallo de las salvaguardas o una situación desconocida hasta el momento y que puede ser relevante para la seguridad.
Gestión de riesgos	Actividades coordinadas para dirigir y controlar una organización

[1] Tomadas del documento ISO/IEC 27001:2005.

	con respecto a los riesgos.
Incidente de seguridad de la información.	Un único evento o una serie de eventos de seguridad de la información, inesperados o no deseados, que tienen una probabilidad significativa de comprometer las operaciones empresariales y de amenazar la seguridad de la información.
Integridad.	La propiedad de salvaguardar la exactitud y completitud de los activos.
Riesgo residual.	Riesgo remanente que existe después de que se hayan tomado las medidas de seguridad.
Seguridad de la información.	La preservación de la confidencialidad, la integridad y la disponibilidad de la información, pudiendo, además, abarcar otras propiedades como la autenticidad, la responsabilidad, la fiabilidad y el no repudio.
Sistema de Gestión de la Seguridad de la Información (SGSI). *Information Security Management System (ISMS).*	La parte del sistema de gestión general, basada en un enfoque de riesgo empresarial, que se establece para crear, implementar, operar, supervisar, revisar, mantener y mejorar la seguridad de la información.
Tratamiento de riesgos	El proceso de selección e implementación de medidas encaminadas a modificar los riesgos.

3.2. Marco de referencia.

La norma ISO 27001 se ha elaborado tomando en consideración el enfoque orientado a procesos y sigue el modelo PDCA para estructurar todos los procesos del SGSI de forma que resulta compatible con las normas ISO 9001 e ISO 14001. Así mismo se contemplan los principios definidos en las Directrices de la OCDE para la Seguridad de los Sistemas y Redes de Información (2002).

Se define **proceso** como:

> ***Conjunto de actividades que utiliza recursos y se gestiona de modo que permite la transformación de unos elementos de "entrada" en unos elementos de "salida".***

En consecuencia, el **enfoque por procesos** consiste en:

> ***"La aplicación de un conjunto de procesos en una organización, junto con la identificación de estos, sus interacciones y su gestión".***

El modelo PDCA (***P****lan*-***D****o*-***C****heck*-***A****ct*) propuesto por Deming (1986) es una estrategia de mejora continua de la calidad en cuatro pasos. Se trata de un proceso cíclico (también conocido como espiral de Deming) que consta de cuatro fases:

- *PLAN* (Planificar): Establecer los objetivos y procesos necesarios para obtener los resultados de acuerdo con el resultado esperado. Al tomar como foco el resultado esperado, difiere de otras técnicas en las que el logro o la precisión de la especificación es también parte de la mejora.
- *DO* (Hacer). Implementar los nuevos procesos. Si es posible, en una pequeña escala.

- *CHECK* (Verificar):

- Pasado un periodo de tiempo previsto de antemano, volver a recopilar datos de control y analizarlos, comparándolos con los objetivos y especificaciones iniciales, para evaluar si se ha producido la mejora esperada.
- Documentar las conclusiones.
  - *ACT* (Actuar):
- Modificar los procesos según las conclusiones del paso anterior para alcanzar los objetivos con las especificaciones iniciales, si fuese necesario.
- Aplicar nuevas mejoras, si se han detectado errores en el paso anterior.
- Documentar el proceso.

A continuación se muestra la adaptación del modelo de Deming al caso de un SGSI:

Planificar (***Plan***) Crear el SGSI	Definir la política, objetivos, procesos y procedimientos del SGSI relevantes para gestionar el riesgo y mejorar la seguridad de la información, con el fin de obtener resultados acordes con las políticas y objetivos generales de la organización.
Hacer (***Do***) Implementar y operar	Implementar y operar la política, controles, procesos y procedimientos del SGSI.
Verificar (***Check***) Supervisar y revisar	Evaluar y, en su caso, medir el rendimiento del proceso contra la política, los objetivos y la experiencia práctica del SGSI, e informar de los resultados a la Dirección para su revisión.
Actuar (***Act***) Mantener y mejorar	Adoptar medidas correctivas y preventivas, en función de los resultados de la auditoría interna del SGSI y de la revisión por parte de la Dirección, o de otras informaciones relevantes, para lograr la mejora continua del SGSI.

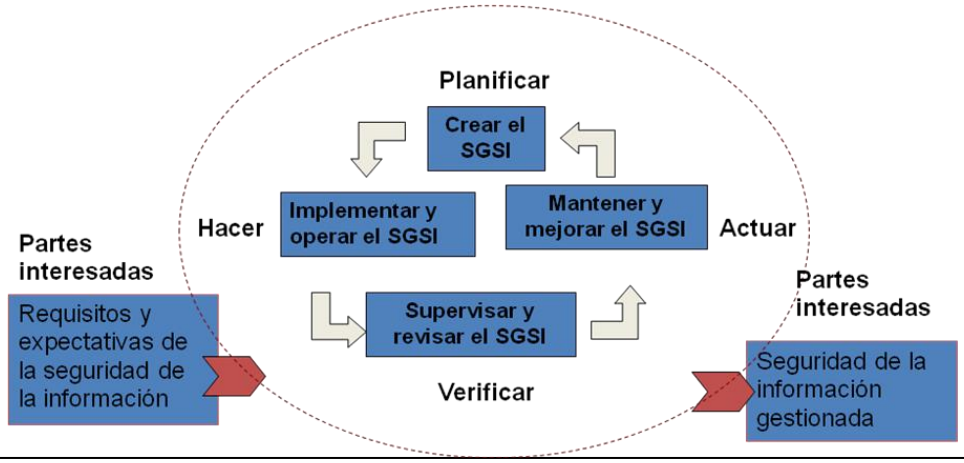

Figura 1. Modelo PDCA aplicado a los procesos del SGSI.

3.3. Estructura de la norma.

La norma UNE-ISO/IEC 27001:2005 se estructura en:

- Un prólogo.
- Cuatro capítulos introductorios.
- El desarrollo de la propia norma (capítulos 4 a 8)2.
- Tres anexos
- Un compendio de referencias bibliográficas.

A continuación se muestra el índice de la misma:

Prólogo.

0. Introducción.
1. Objeto y campo de aplicación.
2. Normas para consulta.
3. Términos y definiciones.

4. Sistema de Gestión de la Seguridad de la Información
4.1. Requisitos.
4.2. Creación y gestión del SGSI.
*4.2.1. [Plan] **Creación** del SGSI.* Contempla (entre otros aspectos):
*4.2.2. [Do] **Implementación** y **operación** del SGSI.*
*4.2.3. [Check] **Supervisión** y **revisión** del SGSI.*
*4.2.4. [Act] **Mantenimiento** y **mejora** del SGSI.*
4.3. Requisitos de la documentación.
5. Responsabilidad de la Dirección.
6. Auditorías internas del SGSI.
7. Revisión del SGSI por la Dirección.
8. Mejora del SGSI.

*ANEXO A. **Objetivos de control y controles.***

ANEXO B. Los principios de la OCDE y esta norma.

ANEXO C. Correspondencia entre esta norma y las ISO 9001 y 14001.

Figura 2. Estructura de la norma ISO 27001.

Las partes más significativas en relación con la presente Guía son la cláusula 4.2 "*Creación y gestión del SGSI*" (que contempla el modelo de Deming) y el anexo A "*Objetivos de control y controles*" que se desarrolla en la norma ISO 27002.

[2] Para obtener la oportuna certificación es obligatoria la aplicación (sin exclusiones) de todos ellos.

3.4. Responsabilidades de la Dirección.

La implicación de la Alta Dirección es, tal vez, el factor más importante para la implantación con éxito de un SGSI. Ésta deberá materializarse en aspectos tales como (cláusula 5 de la norma):

- Formular y aprobar la política del SGSI y difundirla a la totalidad de los miembros de la organización, así como, en su caso, a proveedores y clientes.
- Asignar los roles y responsabilidades a la personal implicado en seguridad de la información.
- Proporcionar los recursos necesarios y asegurar que se implantan programas de concienciación, formación y capacitación.
- Decidir los criterios de aceptación del riesgo y los niveles aceptables de riesgo.
- Autorizar la implementación y operación del SGSI.
- Dirigir las revisiones periódicas del SGSI y velar por la realización de las auditorías internas.

3.5. Documentación del SGSI.

La norma recoge en su cláusula 4 los principales documentos y registros que deben generarse y mantenerse. Básicamente se trata los siguientes:

- Declaraciones de política [4.2.1 b)] y objetivos.
- Alcance del SGSI [4.2.1 a)].
- Procedimientos y mecanismos de control que soporta el SGSI.
- Metodología de evaluación de riesgos [4.2.1 c)].
- Informe de evaluación de riesgos [4.2.1 c), 4.2.1 d), 4.2.1 e), 4.2.1 f) y 4.2.1 g)].
- Plan de tratamiento de riesgos [4.2.2 b)].
- Procedimientos de procesos de seguridad y medida de controles [4.2.3 c)].
- Registros de desarrollo del proceso y de incidentes de seguridad [4.3.3].
- Declaración de aplicabilidad [4.2.1 j)].

La norma establece asimismo consideraciones relativas al control de dichos documentos y registros.

4. ESTRUCTURA DE UN PROYECTO DE IMPLANTACIÓN DE UN SGSI.

En relación con el Sistema de Gestión de la Seguridad de la Información puede hablarse de dos situaciones:

a) El **desarrollo** del sistema. Define el proyecto en sentido estricto. Para ello tiene especial relevancia el apartado 4.2.1 de la norma ISO 27001 "Creación del SGSI" que se corresponde con la fase *Plan* (Hacer) del modelo PDCA en que se consideran, entre otros, los siguientes aspectos:
   - La formulación de la política general de seguridad de la información y de las políticas específicas, así como la redacción de los procedimientos operativos.
   - La elección de una metodología de evaluación de riesgos[3].
   - La realización del análisis de riesgos.
   - La selección los objetivos de control y controles para el tratamiento de los riesgos (Anexo A de la norma, desarrollados en la 27002).
   - Elaborar una declaración de aplicabilidad (SOA).

b) El sistema en funcionamiento (***producción***). Con el sistema implantado deberá realizarse un seguimiento de su eficacia (medición de los controles establecidos, revisión por parte de la Dirección, realización de auditorías internas a intervalos planificados, etc.) con la finalidad de emprender acciones preventivas y correctivas, así como para identificar oportunidades de mejora (cláusula 8) de la norma. A la vista de todo ello se actualizará la documentación del sistema (fundamentalmente en lo que se refiere al análisis de riesgos y a los planes de seguridad) en consonancia con el modelo PDCA.

Un proyecto de SGSI (*crear, implementar, operar, supervisar, revisar, mantener y mejorar un SGI documentado*) puede dirigirse, como cualquier otro, siguiendo los principios del PMI BOK Guide (2004) y consta de las siguientes actividades:

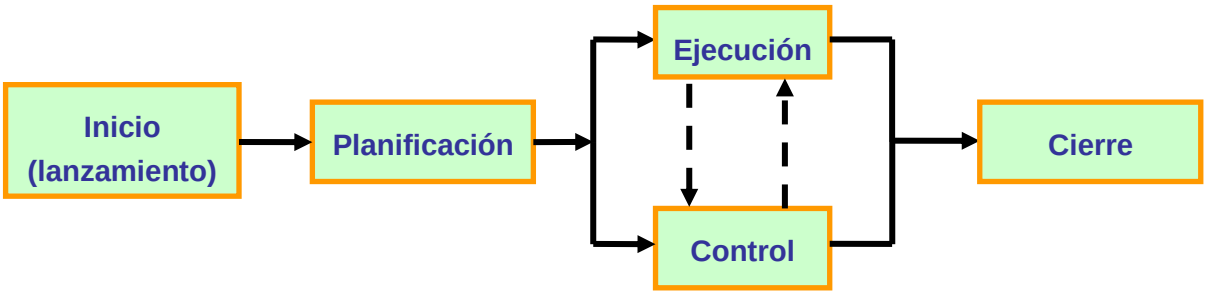

Figura 3. Procesos (fases) de un proyecto SGSI.

Abordamos, a los efectos de la presente guía, únicamente algunos de los aspectos más reseñables de los procesos de inicio y planificación.

[3] MAGERIT es una metodología de análisis y gestión de riesgos propuesta por el Consejo Superior de Administración Electrónica (Ministerio de Hacienda y Administraciones Públicas).

4.1. Procesos iniciales.

4.1.1. Proceso I. Inicio.

Se elabora la **definición del proyecto** (*project charter)* que es un documento de alto nivel que contiene elementos tales como los objetivos, el alcance, la justificación, los participantes (fundamentalmente su director), el presupuesto, la duración etc.

Merece especial atención la constitución del **equipo de proyecto** en el que suele ser habitual la participación de consultores que colaboren con las personas del cliente. El éxito del proyecto dependerá en gran medida de una correcta selección de dicho equipo.

La configuración de un equipo de proyecto es muy variable y depende en gran medida de la madurez de la Organización en cuanto a Seguridad de la Información.

Si la Organización es muy madura dispondrá de un conjunto de figuras similar al que se cita en la guía STIC 801:

- Responsable de la información (***CIO***: ***C****hieff* ***I****nformation* ***O****fficer*).
- Responsable del servicio.
- Responsable de la seguridad de la información (***CISO***: ***C****hieff* ***I****nformation* ***S****ecurity* ***O****fficer*).
- Responsable del sistema [Responsable TIC].
- Responsable de la seguridad del Sistema [STIC: Seguridad TIC].
- Administradores y operadores.
- Así como un órgano colegiado: el **Comité de Seguridad de la Información.** y, tal vez, un **Comité de Seguridad Corporativa.**

No obstante, no es ésta la situación habitual en muchas organizaciones que, por otro lado, resulta impensable para las PYMES, siendo frecuente la figura de un responsable TIC que actúa de forma más o menos coordinada con la Dirección. En tales casos se recomendará encarecidamente una **separación de funciones** entre el **responsable de la seguridad del sistema** (con orientación tecnológica) y (creando, en su caso, tal figura) el **responsable de seguridad de la información** (***CISO***, con visión orientada al negocio).

En cuanto a lo que se refiere al equipo de proyecto de implantación de un SGSI, MAGERIT propone[4] la siguiente estructura de roles y responsabilidades:

[4] Si bien lo hace para los procesos de análisis y gestión de riesgos, puede hacerse extensiva para el proyecto SGSI en su conjunto.

- LA DIRECCIÓN. La Alta Dirección debe actuar como motor e impulsor del proyecto buscando la implicación de todos los participantes, y del resto de la Organización en su conjunto, así como proporcionar los medios (humanos, materiales y económicos) necesarios para la ejecución con éxito del mismo.

- ÓRGANOS COLEGIADOS.
    - **Comité de Dirección**. *Asigna los recursos necesarios para la ejecución del proyecto y aprueba los resultados finales de cada proceso***.** Estará constituido por personas con un nivel alto en la dirección de la Organización, conocimiento de los objetivos estratégicos y de negocio que se persiguen y autoridad para validar y aprobar cada uno de los procesos realizados durante el desarrollo del proyecto.
    - **Comité de Seguimiento**. *Es el encargado de resolver las incidencias surgidas durante el desarrollo del proyecto así como de asegurar la disponibilidad de recursos humanos con los perfiles adecuados y su participación en las actividades donde es necesaria su colaboración y de aprobar los informes intermedios y finales de cada proceso para su elevación al Comité de Dirección.* Está constituido por los responsables de las unidades afectadas por el proyecto así como por los responsables de la informática y de la gestión dentro de dichas unidades. También será importante la participación de los servicios comunes de la Organización (planificación, presupuesto, recursos humanos, administración, etc.). En cualquier caso la composición del comité de seguimiento depende de las características de las unidades afectadas.
    - **Equipo de proyecto**. *Deberá llevar a cabo las tareas del proyecto, recopilar, procesar y consolidar datos y elaborar los informes*. Formado por personal experto en tecnologías y sistemas de información y personal técnico cualificado del dominio afectado, con conocimientos de gestión de seguridad en general y de la aplicación de la metodología de análisis y gestión de riesgos en particular. Si el proyecto se hace con asistencia técnica mediante contratación externa, el subsiguiente personal especialista en seguridad de sistemas de información se integrará en este equipo de proyecto.
    - **Grupos de Interlocutores**. Usuarios representativos dentro de las unidades afectadas por el proyecto en varios subgrupos:
        - Responsables de servicio, conscientes de la misión de la Organización y sus estrategias a medio y largo plazo.
        - Responsables de servicios internos.

  - Personal de explotación y operación de los servicios informáticos, conscientes de los medios desplegados (de producción y salvaguardas) y de las incidencias habituales.

- ORGANOS UNIPERSONALES.
  - **Promotor**. *Es una figura singular que lidera las primeras tareas del proyecto, perfilando su oportunidad y alcance para propiciar su lanzamiento*. Debe ser una persona con visión global de los sistemas de información y su papel en las actividades de la Organización, sin necesidad de conocer los detalles, pero sí al tanto de las incidencias.
  - **Director del Proyecto**. *Es la cabeza visible del equipo de proyecto*. Debe ser un directivo de alto nivel, con responsabilidades en seguridad dentro de la Organización, de sistemas de información o, en su defecto, de planificación, de coordinación o de materias, servicios o áreas semejantes.
  - **Enlace operacional**[5]. *Es el interlocutor visible del Comité de Seguimiento*. Será una persona de la Organización con buen conocimiento de las personas y de las unidades implicadas en el proyecto, que tenga capacidad para conectar al equipo de proyecto con el grupo de usuarios.

En este proceso debe quedar claramente identificado el **alcance** del SGSI así como el tiempo y el coste estimados y, los resultados (entregables – *deliveries*) a obtener, normalmente:

- Documento de política de seguridad de la información.
- Inventario de activos.
- Análisis de riesgos y metodología aplicada.
- Plan(es) de tratamiento de riesgos.
- Declaración de aplicabilidad (***SoA***).
- Selección, implantación de controles y medidas de su eficacia.
- Planes e informes de de auditoría.
- [En su caso] Documento de certificación.

[5] Conviene recordar que un proyecto SGSI siempre es mixto por su propia naturaleza; es decir, requiere la colaboración permanente de especialistas y usuarios tanto en las fases preparatorias como en su desarrollo. La figura del enlace operacional adquiere una relevancia permanente que no es habitual en otro tipo de proyectos más técnicos.

4.1.2. Proceso II: Planificación.

Se contemplan diferentes áreas de gestión (subprocesos): especificación y definición del alcance, actividades (definición, duración y secuenciamiento), asignación de recursos, estimación de recursos, organización, gestión del riesgo (del proyecto), etc.

Algunos de los documentos más importantes generados en este proceso son los siguientes:

- Estructuras de descomposición del trabajo (EDT –***WBS***) y descomposición organizativa (EDO – ***OBS***).
- Planificación temporal. Típicamente un diagrama de Gantt.

La figura siguiente ilustra un ejemplo de WBS acorde con el modelo PDCA[6]

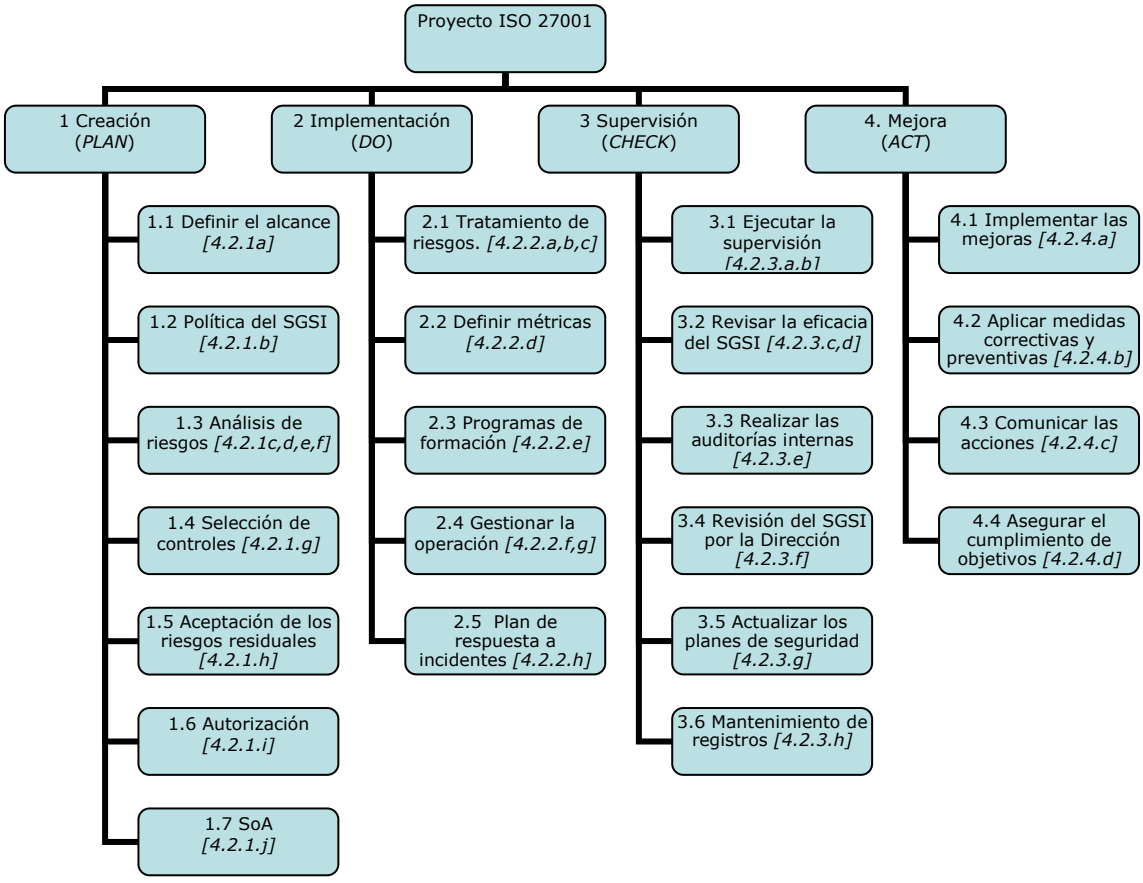

Figura 4. WBS de un SGSI *(Adaptado de Henning 2008)*

A cada una de las tareas (susceptibles de descomposición en mayor grado de detalle) indicadas se le asignará duración, coste, responsables y recursos, así como

[6] Entre corchetes las referencias a las cláusulas de la norma.

las relaciones de precedencia necesarias (pudiendo realizarse algunas de ellas en paralelo). Con la consideración de todo ello podrán elaborarse la planificación y el calendario del proyecto definiendo de manera explícita los conjuntos de entregables que identifican las finalizaciones de los hitos correspondientes.

4.2. Consideraciones económicas.

La elaboración del presupuesto de un proyecto de implantación (y, en su caso, posterior certificación) de un SGSI no resulta nada sencillo dadas la juventud de la norma y el momento de incertidumbre económica en que nos encontramos.

Con anterioridad a la elaboración del mismo convendría identificar algunos aspectos contextuales tales como:

- El grado de implicación de la Alta Dirección.
- El tamaño de la Organización.
- Su cultura, sector productivo y entorno en general.
- Su madurez en tecnologías de la información y comunicaciones.

A la vista de todo ello el principal factor clave de éxito será el acierto en la formulación del **alcance** del proyecto que recomendamos encarecidamente se circunscriba exclusivamente a un número muy reducido de procesos de negocio (a ser posible uno solo) u otro tipo de activos (por ejemplo un CPD).

Esta observación suele constituir un momento delicado en las conversaciones preliminares con el cliente (habitualmente desconocedor de la problemática asociada a la implantación de la norma) pues tal vez se sienta decepcionado al entender que se le desaconseja "*securizar todo*" como le hubiera gustado. El consultor debe tratar de convencerle de acometer inicialmente un proyecto "poco ambicioso" y continuar más adelante con otros.

Con ello se trata de plantear un proyecto asumible en un plazo de tiempo corto[7] (4-6 meses) y con un coste "razonable" (entre 6.000 € y 18.000). Dado que la mayor parte de dicho coste sería imputable a servicios de consultoría (salvo que hubiera que hacer transformaciones tecnológicas importantes) estaríamos hablando de esfuerzos de entre 60 y 180 horas (suponiendo un coste medio de 100 €/h por persona).

A ello habría que añadir (si procede) la auditoría de certificación que se suele calcular en base a una fórmula que incluye al personal implicado directa e

[7] Entiéndase a título de referencia y para el caso de empresas pequeñas y/o alcances limitados, en otros casos estos valores serían más altos. Consideración especial merece la alternativa de una asistencia más personalizada con personal de la consultora "*in house*": las horas de consultoría serían muy elevadas pero, a cambio, desparece casi por completo la dedicación del personal propio de la Organización.

indirectamente. El tiempo mínimo es de 3,5 jornadas y la jornada puede estimarse en torno a los 850 € + gastos (comidas y desplazamiento).

Un vez realizada esta primera aproximación que, además de las consideraciones intrínsecas al propio proyecto, no deberá perder de vista otros factores de entorno tales como el interés del cliente, su disponibilidad presupuestaria, los precios de la competencia y la productividad (basada en la experiencia) del equipo de proyecto podrá procederse a un ajuste más fino tomando en consideración parámetros tales como:

- La información y los servicios (procesos de negocio) implicados.
- El número de activos a valorar.
- El tamaño del equipo del proyecto.
- La complejidad de la estructura organizativa.
- La arquitectura tecnológica.
- La cuantía de procesos externalizados[8] (*outsourcing, hosting, housing, cloud computing*, etc.)

4.3. Herramientas de soporte.

Como consecuencia de las grandes cantidades de datos y de documentos que hay que manejar en los sistemas de gestión de la seguridad de la información se hace prácticamente indispensable el uso de algún tipo de herramienta informática como soporte[9].

Por otro lado, la creciente expansión de las actividades relacionadas con la gestión de la seguridad de la información ha propiciado la aparición de un número importante (que continúa en aumento) de ellas. Algunas referencias pueden encontrarse en ENISA (http://rm-inv.enisa.europa.eu/rm_ra_tools.html) o en el portal ISO 27001 en Español (http://www.iso27000.es/herramientas.html).

Las figuras siguientes muestran, a título de ejemplo, el aspecto de dos herramientas comerciales:

[8] La tendencia al uso de este tipo de servicios externos dado su menor coste no debe llevar a perder de vista el control de la seguridad de la información. "***La responsabilidad ni se delega ni se comparte***".

[9] Nos referimos exclusivamente a herramientas para el soporte de la gestión. Otro tipo de herramientas "*tecnológicas*" (detección de intrusiones, analizadores de red, detectores de vulnerabilidades, antivirus, análisis forense, etc.) caen fuera del alcance de esta guía.

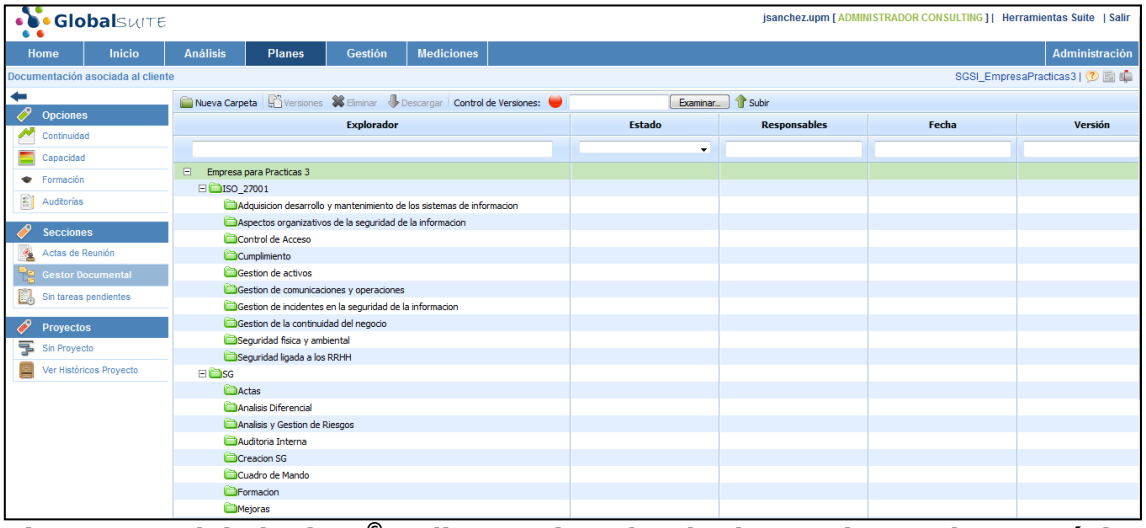

Figura 5. GlobalSuite ©AudiSec. Ejemplo de herramienta de propósito general.

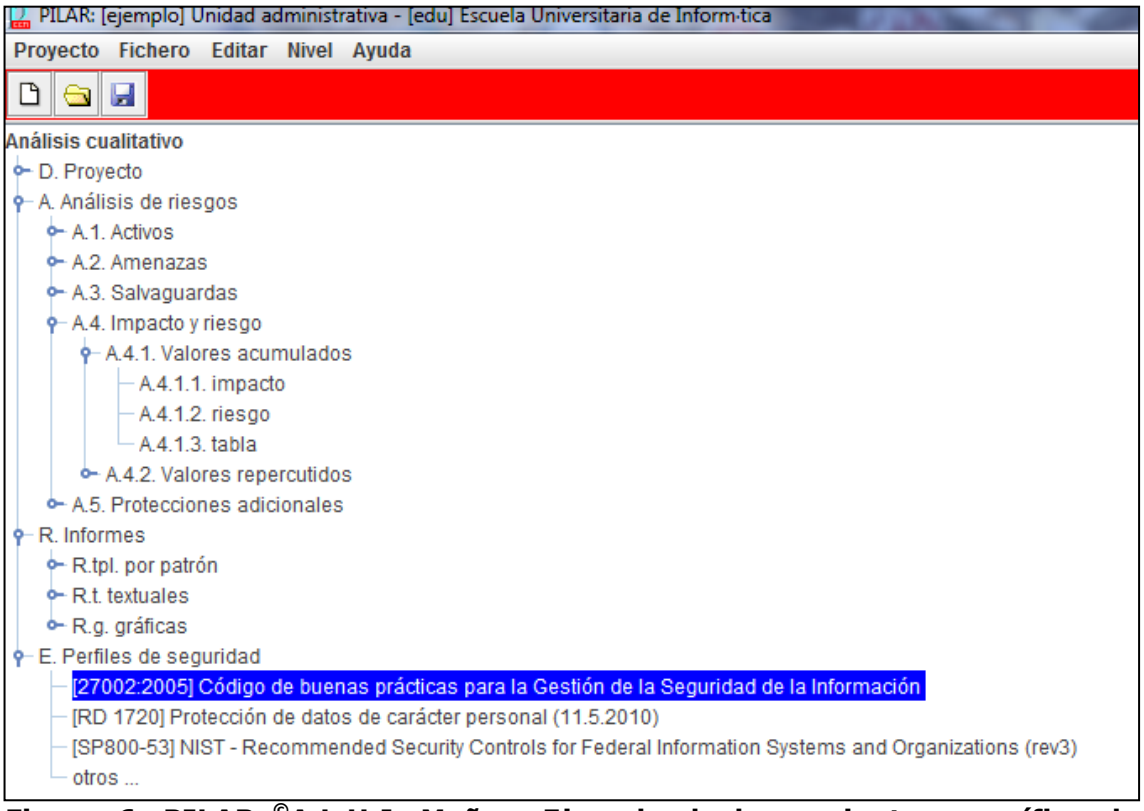

Figura 6. PILAR ©A.L.H.J. Mañas. Ejemplo de herramienta específica de análisis y gestión de riesgos.

5. LOS PROCESOS DE ANÁLISIS Y GESTIÓN DE RIESGOS.

Dado el valor de la información como uno de los activos principales para cualquier Organización (al mismo nivel que otros "clásicos", como los recursos financieros y los humanos) debería ser celosamente "protegida", de manera que se disponga en todo momento de información fiable, puntual y cuya distribución sea controlada adecuadamente.

El concepto de Seguridad Informática | TIC, etc. de la Información, de los Sistemas de Información…) ha evolucionado hacia modelos basados en la **Gestión de Riesgos**, heredados de otros ámbitos (alguno muy antiguo) como, por ejemplo, la salud personal o el transporte público por carretera, que se basan, a grandes rasgos, en la consideración de los siguientes aspectos:

1º) El punto de partida es la concienciación del valor del bien (activo) a proteger.

2º) Como consecuencia de lo anterior se decide aplicar un mecanismo (protocolo).

3º) Es esperable que dicho protocolo esté avalado por instituciones de reconocido prestigio (normalizado).

4º) y siempre aplicando un *principio de proporcionalidad* que tenga en cuenta el equilibrio entre el valor del/los bien/es protegidos y el coste asociado a dicha protección.

Nadie duda que, pese a que tales protocolos sean observados con meticulosidad, en cualquier momento pueda sobrevenir una **contingencia**: enfermedad o accidente de tráfico, en cuyo caso se iniciarían otro tipo de protocolos (hospitalización, pago de indemnizaciones…). En tal caso, **el responsable del servicio o producto quedará liberado**, o al menos, paliado, **de presuntas inculpaciones.**

La Gestión de Riesgos toma como punto de partida la constatación de que **la seguridad absoluta no existe**, por lo que la Dirección deberá asumir unos **niveles de riesgo aceptable**. Queremos resaltar este (evidente) hecho como contrapunto a ciertos planteamientos y actitudes que se observan con demasiada frecuencia. "*Securizar*" es uno de los paradigmas más representativos, que tienden a crear falsas expectativas, con las consiguientes decepciones en clientes desconocedores de la materia.

5.1. Metodologías de análisis y gestión de riesgos.

La aplicación de la norma ISO 27001 requiere que se especifique una metodología de evaluación de riesgos (cláusula 4.2.1c) y que se formule un plan de tratamiento de riesgos (cláusula 4.2.2a).

Existen varias metodologías adecuadas para ello que no difieren en lo sustancial.

Puede encontrarse un inventario de ellas en ENISA (http://rm-inv.enisa.europa.eu/rm_ra_methods.html).

Una de las metodologías más conocidas es MAGERIT[10] desarrollada por el Consejo Superior de Administración Electrónica (CSAE), organismo dependiente del Ministerio de Hacienda y Administración Pública (aunque se la suele identificar con el Ministerio de Administraciones Públicas de quien dependió originalmente).

También, en el catálogo de ENISA se encuentran referencias a herramientas informáticas adecuadas para la aplicación de las correspondientes metodologías. PILAR[11] (***P***rocedimiento ***I***nformático y ***L***ógico para el ***A***nálisis de ***R***iesgos), desarrollada por el Centro Criptológico Nacional, dependiente del Centro Nacional de Inteligencia (CNI) de Presidencia (anteriormente Defensa), es la específica de MAGERIT[12].

5.2. El proceso de análisis de riesgos.

El análisis de riegos consiste en un proceso cuya finalidad es conocer el estado de riesgo a que se encuentra sometido un sistema (proceso de negocio[13]) para que la Dirección pueda tomar las decisiones oportunas. Aunque puede diferir ligeramente de unas metodologías a otras, se basa en los principios siguientes:

- **El objeto a proteger** (**activo**). Se conoce como activo "todo aquello que tiene la Organización, cuya pérdida o deterioro causaría un perjuicio". La naturaleza de los activos es muy diversa, algunos son tangibles (por ejemplo: un Centro de Proceso de Datos) en tanto que otros son intangibles (ejemplos: un servicio proporcionado por la Organización o una información importante para su actividad). **Estos últimos suelen ser los más importantes**.
- **Las dimensiones de la protección** (**seguridad**). Identificadas popularmente bajo el acrónimo ***ACID*** (***A***utenticidad, ***C***onfidencialidad, ***I***ntegridad, ***D***isponibilidad)[14].

---

10 http://administracionelectronica.gob.es/?_nfpb=true&_pageLabel=PAE_PG_CTT_General&langPae=es&iniciativa=184#PAE_12946627283622722

11 https://www.ccn-cert.cni.es/index.php?option=com_wrapper&view=wrapper&Itemid=187&lang=es

12 PILAR es una herramienta muy utilizada y referenciada, aunque se suele criticar su complejidad. Es frecuente escuchar a Organizaciones que empezaron a utilizarla pero han continuado con una versión "recortada". En cualquier caso, en las ofertas de empleo se suele valorar su conocimiento (requisito indispensable en empleo público).

13 Identificado en el alcance del SGSI. Es un error frecuente en los principiantes pensar que se va a abordar la gestión de la seguridad de la información de la totalidad de la Organización.

14 No todas las metodologías contemplan estas dimensiones: algunas excluyen la Autenticidad y, por el contrario, otras incluyen dimensiones adicionales como la trazabilidad o el no repudio. Las dimensiones de Confidencialidad, Integridad y Disponibilidad suelen estar siempre presentes.

Los activos poseen **valores** en sus diferentes dimensiones. Es importante resaltar la acepción que damos al término **valor**: "**La importancia que daríamos a la vulneración de cualquiera las dimensiones de un activo.**" Por ejemplo:

- En la dimensión de **Autenticidad:** *¿Qué perjuicio causaría no saber exactamente quien hace o ha hecho cada cosa*?
- En la dimensión de **Confidencialidad**: *¿Qué daño causaría que conociera un activo quien no debe*?
- En la dimensión de **Integridad**: *¿Qué perjuicio causaría que un dato estuviera dañado o corrupto*?
- En la dimensión de **Disponibilidad**: *¿Qué perjuicio causaría no tener o no poder utilizar un activo*?

El valor de un activo, en su correspondiente dimensión *ACID*, **no se corresponde** necesariamente **con su valor propio** sino con la valoración del daño que produciría a la Organización. Por ejemplo, una avería eléctrica de 24 horas de duración supondría un perjuicio (desde la dimensión de disponibilidad) que sería la suma del propio valor correspondiente a la reparación de la avería, más la de los equipos que eventualmente hayan podido quedar dañados más (y sobre todo) las derivadas de no haber podido facilitar durante ese tiempo los servicios comprometidos. Ello significa que se establece una **dependencia entre activos**, de manera que un activo P (padre) puede depender de otro H (hijo) en el sentido de que si H sufriera un percance, P se vería indirectamente perjudicado.

- **Las amenazas a que están expuestos los activos**. Se definen las amenazas como: "*Eventos que pueden desencadenar un incidente en la Organización, produciendo daños materiales o pérdidas inmateriales en sus activos*". Las diferentes amenazas se caracterizan por dos parámetros:
  - ***Degradación***: Porcentaje en que quedaría afectado el activo en caso de que la amenaza se materializase (0%: el activo no se vería afectado – 100%: el daño seria total).
  - ***Frecuencia***: Tasa anual de ocurrencia de la amenaza (0: nunca va a producirse, 1: una vez al año – 100: se produce a diario).

  Pese a que pueden utilizarse valores numéricos para ambos parámetros en la práctica se prefiere utilizar una valoración por intervalos tal como: {*Muy alta, Alta, Media, Baja*}.

  La materialización de una amenaza implicaría un **impacto** sobre el activo y en la dimensión de seguridad implicados. No obstante se prefiere trabajar con el

concepto de **riesgo** que tiene en cuenta tanto el **impacto** como la **probabilidad** de que materialice la amenaza sobre el activo y en la dimensión de seguridad afectados.

El origen y la naturaleza de las amenazas son diversos. MAGERIT contempla un catálogo (utilizado con frecuencia en otras metodologías) de 58 tipos de amenazas agrupadas en cuatro bloques: [N] Desastres naturales, [I] De origen industrial, [E] Errores y fallos no intencionados, y [A] Ataques deliberados

La consideración conjunta de todos estos aspectos genera una información (por lo general bastante voluminosa) conocida como ***mapa*** o ***estado de riesgo*** a partir de cuya consideración la Dirección (esta responsabilidad es indelegable) deberá decidir, para cada uno de los riesgos, si:

- Rechazarlo. "No viajar en avión para evitar el riesgo asociado".
- Asumirlo.
- Transferirlo. La solución más frecuente en este sentido es la contratación de una póliza de seguros.
- **Gestionarlo** (gestión de riesgos). Lógicamente esta alternativa es la que ofrece más posibilidades.

5.3. El proceso de Gestión de riesgos.

Para reducir un riesgo hay que actuar sobre las **vulnerabilidades** identificadas a base de implantar mecanismos de **salvaguarda** o **controles**[15] que, una vez aplicadas consiguen reducir el riesgo a un valor (**residual**[16]) que la Dirección deberá nuevamente conocer para decidir si asumirlo o, por el contrario, continuar mejorando las salvaguardas (lo que, obviamente, supone un coste).

Las salvaguardas actúan sobre las amenazas reduciendo la degradación y/o la probabilidad.

No hay que pensar que todas las salvaguardas son de tipo técnico, también las hay organizativas y físicas. Por ejemplo:

- La instalación de un antivirus (técnica) sería efectiva frente a la amenaza de difusión de software dañino [E.8 | A.8] en el sentido de reducir su frecuencia (aunque no tendría efectos sobre la degradación).
- La implantación de un procedimiento gestionado para la realización de copias de

[15] En organizaciones maduras la mayoría de los controles tecnológicos ya están implantados. Lo que no es tan frecuente es que se disponga documentalmente de la medida de su eficacia, de la existencia de procedimientos de mejora continua así como de otros controles no tecnológicos, especialmente la formación y concienciación.

[16] Reiteramos el principio de que **la seguridad absoluta no existe**.

seguridad (organizativa / técnica) reduciría el impacto (pero no la frecuencia) de las amenazas de degradación [E.17] o pérdida [E.18] de información.

Existen diferentes conjuntos de controles/salvaguardas tales como los recogidos en el anexo A de la norma ISO 27001 (que se desarrolla en la norma ISO 27002), las medidas de seguridad del Esquema Nacional de Seguridad, la norma NIST 800-53, las contempladas en el RD 1720/2007 para el caso específico de protección de datos de carácter personal, etc.

La relación de controles / salvaguardas que vaya a ser considerada debe recogerse en documento denominado ***Declaración de Aplicabilidad*** (***SOA***) **del que se hace responsable la Alta Dirección**.

Los procesos de análisis y gestión de riesgos no son independientes sino que interactúan tal como se ilustra en la figura siguiente.

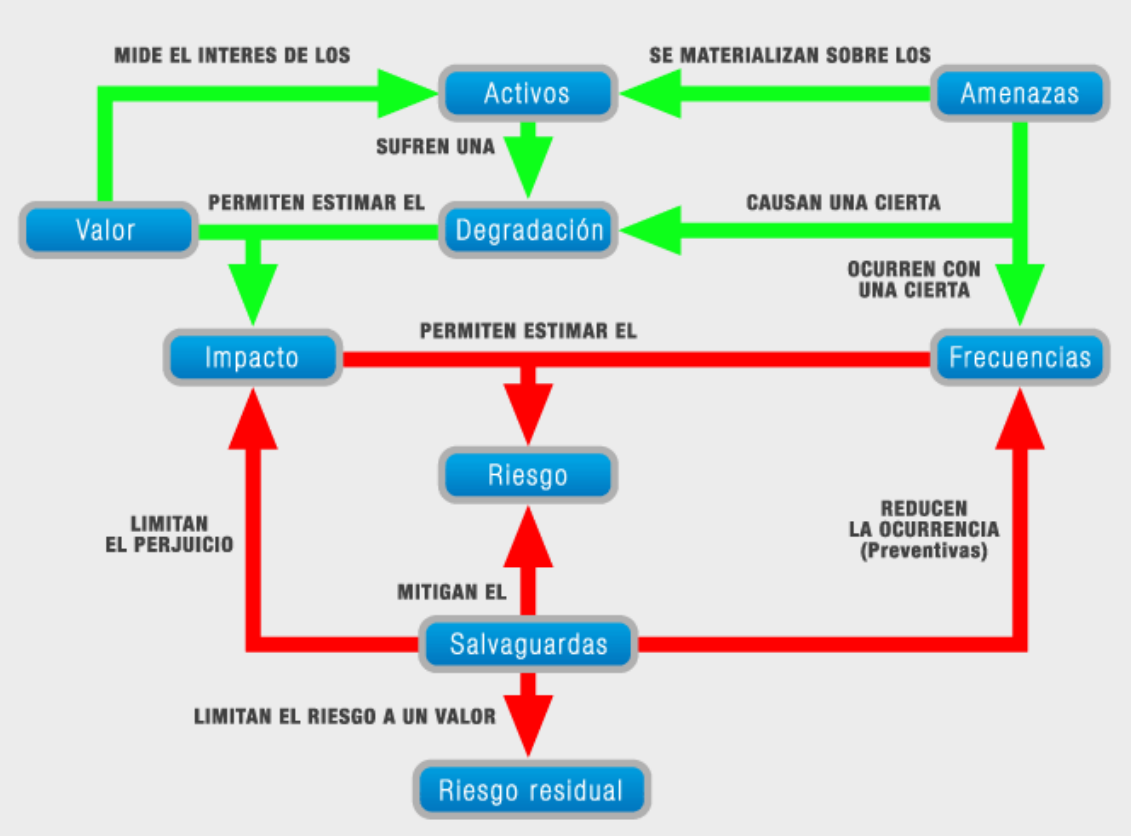

Figura 7. Esquema del método MAGERIT *(fuente ccn-cert)*

Con las decisiones que se adopten se formulará un plan de actuación que deberá contemplar: objetivos, responsables, recursos, plazos, etc., así como un conjunto de **métricas** de para evaluar la **eficacia de los controles** una vez que se haya implantado el sistema. Los resultados obtenidos se tomarán en consideración para la introducción de nuevas mejoras siguiendo el modelo PDCA.

6. CONTROLES.

La aplicación de la norma ISO 27001 requiere seleccionar un conjunto de objetivos de control y controles (cláusula 4.2.1 *g*) que deberán ser implantados (cláusula 4.2.2 *c*) y evaluados con posterioridad como consecuencia del proceso de supervisión y revisión del SGSI (cláusula 4.3.2. *c*) para ver si se alcanzan los criterios de aceptación de riesgo y dar así cumplimiento a los objetivos del proceso de mejora continua (cláusula 4.2.4).

La norma ISO 27002:2005[17] (anteriormente 17799): "*Código de buenas prácticas para la gestión de la seguridad de la información*" desarrolla el Anexo A de la norma ISO 27001 proporcionando asesoramiento para su implantación.

Se define **control** (sinónimo de salvaguarda o contramedida) como:

> ***"Medio de gestión del riesgo que incluye políticas, procedimientos, directrices, prácticas o estructuras de la organización que pueden ser de naturaleza administrativa, técnica, de gestión y legal".***

Se presenta un conjunto de 133 controles, agrupados en 39 objetivos de control que lo hacen, a su vez, en 11 dominios. En la práctica las organizaciones podrán excluir algunos o añadir otros siempre que se justifique adecuadamente. El documento que contempla la totalidad de controles seleccionados y su justificación se denomina **Declaración de Aplicabilidad** (***SOA***).

El texto de la norma ISO 27002:2005 está organizado en base a:

- Una parte introductoria (prólogo y capítulos 0 a 4).

  En el capítulo 0 (Introducción) se presentan cuestiones generales tales como: el concepto y la justificación de la seguridad de la información, los principios de la aplicación de controles para la gestión de la seguridad de la información, la exposición de un conjunto básico de controles como punto de partida, los factores críticos de éxito y sugerencias para el desarrollo de directrices propias.

  El conjunto básico de controles está constituido por:

  - Controles exigibles por la legislación:
    a) La protección y la privacidad de la información de carácter personal (control 15.1.4).
    b) La protección de los registros de la organización (control 15.1.3).
    c) Los derechos sobre la propiedad intelectual (control 15.1.2).
  - Controles considerados como "las mejores prácticas" (*best practices*):

[17] La norma ISO 27002 no es certificable.

a) El documento de política de seguridad de la información (control 5.1.1).
b) La asignación de responsabilidades de seguridad de la información (control 6.1.3).
c) La concienciación, formación y capacitación en seguridad de la información (control 8.2.2).
d) El procesado correcto en las aplicaciones (objetivo de control 12.2).
e) La gestión de las vulnerabilidades técnicas (objetivo de control 12.6).
f) La gestión de la continuidad del negocio (dominio 14).
g) La gestión de los incidentes y las mejoras en seguridad de la información (objetivo de control 13.2).

El capítulo 1 identifica el objeto y campo de aplicación de la norma.

El capítulo 2 incluye el glosario de términos que se ha recogido en el apartado anterior.

El capítulo 3 explica la estructura de la norma (capítulos 5 a 15).

El capítulo 4 profundiza en los conceptos de **evaluación** y **tratamiento** de los riesgos de seguridad. La **evaluación** del riesgo incluye la aproximación sistemática para estimar su magnitud (análisis de riesgos) y el proceso de comparar los riesgos estimados con los criterios de aceptabilidad. Para cada uno de los riesgos identificados es necesario realizar un **tratamiento** específico. Se plantean cuatro opciones posibles:

- **Aplicar** / mejorar los **controles** apropiados para reducir los riesgos. Esta opción representa el tratamiento en sentido estricto.
- **Aceptar** consciente y objetivamente del riesgo.
- **Evitar** el riesgo.
- **Transferir** el riesgo a otras partes, por ejemplo aseguradoras o proveedores.

- El propio contenido de la norma (capítulos 5 a 15).

  Cada uno de los capítulos se corresponde con un **dominio de control** que se subdivide en un conjunto de **objetivos de control** que, a su vez, contemplan uno o varios **controles**.

  Para cada control la guía proporciona su definición, recomendaciones para su implementación y, en algunos casos, otra información adicional.

- Un compendio de referencias bibliográficas.

La figura siguiente constituye una aproximación de primer nivel (dominios). Como puede apreciarse solo cuatro de ellos contemplan aspectos técnicos y tecnológicos: Seguridad física y del entorno (9), Gestión de comunicaciones y operaciones (10), Control de accesos (11) y Adquisición, desarrollo y mantenimiento de los sistemas

de información (12) en tanto que el resto (7) de los dominios se ocupan de consideraciones organizativas y legales.

Figura 8. Dominios de la norma ISO 27002 y su naturaleza.

Fuente (http://www.unit.org.uy/iso27000/iso27000.php)

7. CERTIFICACIÓN DE UN SGSI.

7.1. Esquema de certificación.

Se entiende por certificación:

> *"El Proceso mediante el que un organismo certificador (acreditado) da garantía escrita de que un producto, proceso o servicio es conforme con unos requisitos (normas o estándares) específicos*

La obtención (y conservación) de una certificación faculta a la **empresa certificada** a exhibir un sello distintivo. La figura siguiente muestra algunos conocidos ejemplos.

Figura 9. Ejemplos de marcas de certificación.

La certificación de una empresa según la norma ISO 27001 se obtiene después de que una **entidad de certificación** realice, con resultados satisfactorios, una auditoría (denominada de "tercera parte") y eleve a un **organismo de acreditación** la correspondiente solicitud favorable.

Las **entidades de certificación** son organismos de evaluación de la conformidad, encargados de realizar una declaración objetiva de que el SGSI opera de acuerdo con la finalidad y objetivos definidos, con la norma ISO 27001 así como con los procedimientos internos y cumple con la legislación aplicable y otras normativas. Estas entidades han de ser neutrales y cumplir con los requisitos de independencia, imparcialidad, competencia e integridad.

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 con diversas entidades certificadoras y solicitar presupuesto por los servicios ofrecidos, comparando y decidiéndose por la más conveniente, como se hace con cualquier otro producto o servicio.

Para que una empresa (entidad de certificación) pueda expedir certificaciones es necesario esté acreditada por un **organismo de acreditación**, que en el caso de

España es la Entidad Nacional de Acreditaciones[18] (ENAC). En otros países existen organismos similares tales como UKAS (Gran Bretaña), RAB (USA), COFRAC (Francia), JISC (Japón), etc. y es frecuente la existencia de acuerdos, de manera que una empresa acreditada puede actuar en diferentes países. El ***IAF*** (***I****nternational* ***A****ccreditation* ***F****orum*) establece la regulación a nivel mundial.

Se entiende por acreditación:

> *"El procedimiento mediante el cual un organismo autorizado (en España, ENAC) reconoce formalmente que una organización es competente para la realización de una determinada actividad de evaluación de la conformidad (organismo certificador).*

La figura siguiente ilustra esquemáticamente la relación entre los conceptos expuestos:

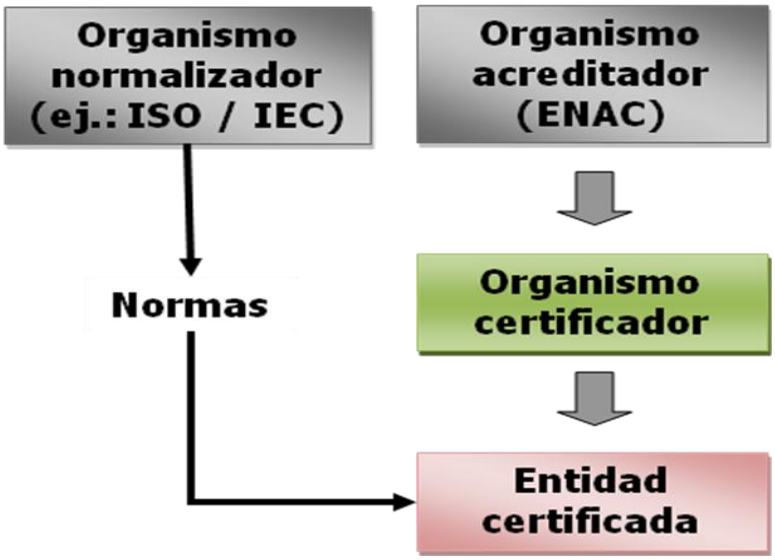

Figura 10. Normalización, acreditación y certificación.

7.2. Proceso de certificación.

Una vez que se dispone de un SGSI implantado y funcionando, el siguiente paso será certificarlo (si se desea hacerlo).

La certificación consiste en la obtención de un documento que reconoce y avala la correcta adecuación del mismo a esta norma. En cualquier caso **el hecho de certificar un SGSI no implica garantizar la seguridad de la información ni las medidas de seguridad implantadas**, lo que se certifica es ***proceso*** bajo el

[18] En la siguiente dirección de ENAC en Internet puede encontrarse una relación de empresas acreditadas para dicha certificación: http://www.enac.es/web/enac/acreditados.

que se realiza la gestión del sistema de seguridad de la información (de la misma forma que la certificación ISO 9001 no garantiza la calidad de los ***productos*** o ***servicios*** sino el proceso de gestión de la ***calidad***).

Para certificar un SGSI hay que acudir a una **entidad de certificación** (lo natural será solicitar varias ofertas y seleccionar la más adecuada).

La entidad de certificación solicitará de la organización aspirante a la certificación la existencia previa de:

- Un SGSI según la norma ISO 27001 implantado y funcionando durante un tiempo suficiente (más de 3 meses).
- El análisis de riesgos.
- La realización de la auditoría interna y su revisión por parte de la dirección.

Para verificar todo ello la entidad de certificación enviará a la empresa candidata un cuestionario a partir de cuya valoración considerará si está preparada para afrontar con éxito la **auditoría de certificación**. En caso favorable se realiza dicha auditoría en dos fases[19]:

- Fase 1. Los auditores revisan la documentación del SGSI proporcionada por el cliente. A partir de ella se reflejan hallazgos con los que se prepara un informe. Estos hallazgos pueden ser **Críticos** o **No Críticos** en función de que se serían, respectivamente, motivos de **No Conformidades Mayores** o **Menores** en la fase 2. Se emplaza a la Organización aspirante a la certificación a subsanarlos antes de proceder a ella.

- Fase 2. Los auditores revisan *in situ* las políticas, la implantación de los controles de seguridad y la eficacia del sistema en su conjunto[20]. 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 en donde quedarán reflejadas, entre otros aspectos, la relación de **No Conformidades** (menores y mayores) encontradas así como posibles oportunidades de mejora.

  Para cada una de las **No Conformidades** se elaborará una **Solicitud de Acción**

[19] Se contempla adicionalmente una posible visita de pre auditoría con el objetivo de proporcionar información para la planificación de la auditoría, así como conocer el estado de la Organización para afrontar la auditoría.

[20] En la auditoría no se consideran todos los aspectos (ni, en su caso, todas las ubicaciones), sería inviable. Se realizan técnicas de muestreo.

Correctora (*SAC*) en donde se harán constar aspectos tales como:

- La deficiencia observada y la/s evidencia/s que lo constata/n.
- La/s cláusula/s de la norma afectadas.
- El nombre del auditor-

La Organización auditada deberá elaborar un plan de actuación para subsanar cada una las No Conformidades. En el caso de las menores bastará con que el auditor de su aprobación al plan correspondiente (que deberá estar ejecutado con anterioridad a la próxima auditoría de seguimiento) por el contrario no se propondrá la certificación hasta que no estén corregidas las No Conformidades mayores.

La certificación en la norma ISO 27001 tiene una vigencia de tres años. Para mantenerla se necesita superar una auditoría de renovación así como auditorías de seguimiento (menos exhaustivas) anuales.

7.3. Razones para la certificación.

Pese al coste que lleva consigo, la certificación supone una indudable e importante ventaja competitiva para las empresas que la obtienen dada su capacidad de generar confianza entre sus clientes, proveedores, empleados y financiadores respecto a que las cosas se hacen empleando las mejores prácticas reconocidas en su sector (*lo que no asegura necesariamente que las cosas "salgan bien"*). De alguna manera estamos viviendo una situación similar a la que se encontraba a mediados de las años [19]90 con *el fenómeno web*; "*Hoy supone una ventaja competitiva; mañana, su carencia será una seria desventaja*".

Algunos de los motivos de las organizaciones para obtener dicha certificación pueden ser:

- El prestigio que supone el reconocimiento de que la gestión se está realizando de manera clara y eficaz y siguiendo buenas prácticas internacionales.
- La confianza que genera tanto en el interior de la organización como ante sus clientes y proveedores.
- Mejorar la visibilidad del área de sistemas (TIC) facilitando la comunicación entre dicho área y el resto de la organización.
- Obtener una ventaja competitiva al establecer un factor de diferenciación respecto a otras de la competencia no certificadas. Esta ventaja competitiva puede convertirse en una verdadera barrera cuando los clientes valoran favorablemente (o incluso exigen) en las licitaciones que las organizaciones proveedoras estén certificadas.

8. CONSIDERACIONES PROFESIONALES.

8.1. Tipología de organizaciones ofertantes. (Mercado objetivo).

La norma ISO 27001 es aplicable a todo tipo de organizaciones con independencia de su tamaño y sector de actividad.

Existe una creencia algo generalizada de que el mercado objetivo son las empresas desarrolladoras de productos y servicios TIC. No es cierto dado que el objetivo de la norma es la **seguridad de la información** (en sus múltiples dimensiones) con independencia de la forma en que esta se procese, almacene o transmita. Así habrá que abordar aspectos tales como la seguridad física, la contratación de personal, la destrucción de documentos, las normativas legales (muy en particular la LOPD), etc. y, por supuesto, todo lo relacionado con las TIC's.

Lo habitual es que la implantación de un SGSI según la norma ISO 27001 corra a cargo de un equipo de especialistas en diferentes áreas (algunas de ellas específicas de Ingenieros de Telecomunicación, aunque otras no) si bien el rol de director de proyecto ofrece muchas posibilidades para nuestro colectivo dado que:

- Este segmento de mercado no suele disponer de personal competente para elaborar y mantener sus Sistemas de Gestión de la Seguridad de la Información.
- Es necesario aunar los conocimiento de los procesos de negocio con los de tipo legislativo y tecnologías de la información y las telecomunicaciones. Aunque otros colectivos están más especializados en algunas de ellas no es fácil que lo estén en todas a la vez.
- Además de los conocimientos profesionales se requieren unas habilidades de liderazgo, trabajo en equipo y gestión de proyectos muy valoradas en nuestra profesión.

También puede considerarse como objetivo de mercado las Administraciones Públicas:

- Como motor de iniciativas a consecuencia de las cuales se generan importantes oportunidades de negocio (sirvan como ejemplos el *Esquema Nacional de Seguridad* o el Real Decreto de *Medidas para la Protección de las Infraestructuras Críticas*). En algunos casos tales incitativas adquieren el rango de Ley (Ley Orgánica de Protección de Datos, Ley de Servicios de Sociedad de la Información, Ley de Firma Electrónica, Ley de Administración Electrónica, etc.) que, además de su necesaria observación para no incurrir en responsabilidades administrativas, civiles o penales, también ofrecen oportunidades de negocio en el asesoramiento a organizaciones interesadas en su contemplación.
- En diferentes convocatorias de Oferta de Empleo Público que contemplan en los

temarios de los Concursos y Oposiciones aspectos relacionados total o parcialmente con la seguridad de la información.

8.2. Perfiles profesionales.

La seguridad de la información ofrece diferentes salidas profesionales:

- En organizaciones en general.
  - Las grandes ofertan diversas ofertas de empleo relacionadas con la seguridad de la información: las de perfiles más altos aparecen con términos tales como ***CIO*** (***C****hief* ***I****nformation* ***O****fficer*), ***CISO*** (***C****hief* ***I****nformation* ***S****ecurity* ***O****fficer*), Responsable **STIC** (Seguridad TIC), etc., así como un elevado número de otras tanto con carácter general como vinculadas a tecnologías o productos concretos. También es habitual encontrar en estas organizaciones perfiles de auditor interno.
  - Las pequeñas, que al disponer de plantillas más reducidas, buscan profesionales polivalentes que posean tanto conocimientos tecnológicos como de gestión.
- Las empresas de servicios

  A su vez divididas en consultoras y auditoras. Serán siempre distintas dado que el principio de imparcialidad que se exige a la función auditora impide a una misma empresa realizar ambas actividades.

  Aunque algunos de los requisitos son comunes para consultores y para auditores los de estos últimos suelen ser más rigurosos.

8.2.1. Perfil del auditor de seguridad de la información.

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*.

a) De tercera parte: Auditor externo, normalmente porque la organización tiene la intención de lograr la certificación y contrata para ello los servicios de una entidad de certificación.

Al auditor se le exigen una serie de atributos personales, conocimientos y

habilidades, educación formal, experiencia laboral y formación como auditor.

El auditor, sobre todo si actúa como de tercera parte, ha de disponer también de una certificación personal en la norma ISO 27001. Esto quiere decir que, nuevamente un tercero (acreditador), certifica que posee las competencias profesionales y personales necesarias para desempeñar la labor de auditoría de la materia para la que está certificado además debe poseer conocimientos y experiencia en el sector a auditar (Automoción, TI, Sanitario…).

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.

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 en equipo.

8.3. Requisitos de formación.

Dado que el Estado español no regula facultades para el ejercicio de este tipo de actividades profesionales, el Colegio Oficial de Ingenieros de Telecomunicación solo puede ayudar a los colegiados poniendo a su disposición mecanismos y recursos para la obtención de ventajas competitivas respecto a otros colectivos. (En tal sentido se ha elaborado la presente Guía).

Tampoco la norma ISO 27001 establece requisitos sobre la formación que han de poseer las personas que diseñen e implanten o efectúen las auditorías (internas o externas) de los Sistemas de Gestión de la Seguridad de la Información en las empresas y organizaciones.

Sin embargo, las ofertas de empleo suelen recabar dos tipos de requerimientos (aparte de la experiencia):

- De naturaleza académica.

  Aunque las titulaciones más demandadas suelen ser las Ingenierías de Telecomunicación e Informática es frecuente que la naturaleza de la Ingeniería sea un factor secundario. Lo que busca el empleador es un conocimiento generalista y, sobre todo, las actitudes y capacidades transversales obtenidas

como consecuencia de una formación universitaria.

- De naturaleza profesional:
  - Poseer el conocimiento y compresión de la norma. Para ello es muy conveniente realizar algún curso que además de impartir la enseñanza de las normas, emita un certificado que garantice que el alumno ha finalizado el mismo con aprovechamiento[21]. Dos de las certificaciones más reconocidas a nivel internacional son CISA (ISACA[22]) y Lead Auditor 27001 (IRCA[23]).
  - Tener experiencia en los procesos y funcionamiento de las empresas.
  - Poseer conocimientos de tecnologías y productos específicos.

El siguiente es un ejemplo real (Fuente *Infojobs*) de oferta de empleo de Consultor de Seguridad.

Estudios mínimos:	Ingeniero
Experiencia mínima:	Al menos 3 años
Requisitos mínimos:	Será requisito indispensable la experiencia, de al menos 3 años, en proyectos relacionados con: • Análisis de Riesgos basados en MAGERIT. • Implantación de Planes Directores de Seguridad o SGSI según la norma UNE-ISO/IEC 27001 y/o normativas anteriores, como por ejemplo las normas ISO/IEC 17799, BS 7799.
Requisitos deseados:	• Se valorará la posesión cursos de formación y certificaciones en seguridad en general y, especialmente, en SGSI según la norma UNE-ISO/IEC 27001. • Se valorará positivamente la posesión por parte de los consultores de certificaciones específicas de Seguridad TI. • Se valorará la experiencia en alguna (o varias) de las siguientes materias: o Revisión y Desarrollo de Marco Normativo de Seguridad. o Consultoría para la evaluación de conformidad con la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal (LOPD). o Implantación de otros estándares reconocidos como COBIT, ITIL, NIST, etc. o Utilización de metodología relativa a la protección de la información PCI DSS. o Planes de Continuidad de Negocio.

[21] Además de las organizaciones privadas, las Administraciones Públicas constituyen una importante fuente de oferta formativa de gran calidad y, en muchos casos, con carácter gratuito.

[22] http://www.isaca.org/Certification/CISA-Certified-Information-Systems-Auditor/Pages/default.aspx

[23] http://spain.irca.org/auditorcert.html

9. BIBLIOGRAFÍA Y ENLACES DE INTERÉS.

9.1. Bibliografía

- Análisis y Gestión de Riesgos en los Sistemas de Información (2011). J. Sánchez y otros. Departamento de Publicaciones, EUI-UPM.
- Out of the Crisis (1982) Deming, W. MIT Press.
- Project Management Institute (PMI) (2004). A Guide to the Project Management Body of Knowledge (PMBoK Guide). Philadelphia, Pennsylvania: PMI.
- Tackling ISO 27001: A Project to Build an ISMS. SANS Institute InfoSec Reading Room. (Disponible en Internet: http://www.sans.org/reading_room/whitepapers/leadership/tackling-iso-27001-project-build-isms_33169. Accedido 15-04-2012).
- Directrices de la OCDE para la Seguridad del Información: Hacia una cultura de seguridad. OCDE, 2002. (Disponible en Internet: http://www.oecd.org/dataoecd/15/29/34912912.pdf. Accedido 13-5-2012).
- Norma UNE-EN ISO 27001:2005. Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información (SGSI). Requisitos. AENOR.
- Norma UNE-EN ISO 27002:2009. Tecnología de la Información. Técnicas de seguridad. Código de buenas prácticas para la gestión de la seguridad de la información. AENOR.
- Norma UNE-EN ISO 19011:2012 Directrices para la auditoría de los sistemas de gestión. AENOR.
- Método MAGERIT. (Disponible en Internet: http://administracionelectronica.gob.es/?_nfpb=true&_pageLabel=P8002922512936515509 91&langPae=es&detalleLista=PAE_1276529683497133. Accedido 15-04-2012).
- Ley 11/2007 de acceso electrónico de los ciudadanos a los Servicios Públicos (Disponible en Internet: http://www.boe.es/aeboe/consultas/bases_datos/doc.php?id=BOE-A-2007-12352. Accedido 13-5-2012).
- Esquema Nacional de Seguridad (Disponible en Internet: http://www.boe.es/boe/dias/2010/01/29/pdfs/BOE-A-2010-1330.pdf Accedido 15-04-2012).
- Esquema Nacional de Seguridad. Corrección de erratas. (Disponible en Internet: http://boe.es/aeboe/consultas/bases_datos/doc.php?id=BOE-A-2010-4054.

Accedido 15-04-2012).

- Guías STIC Serie 800 (Disponible en Internet: https://www.ccn-cert.cni.es/index.php?option=com_content&view=article&id=2420&Itemid=211&lang=es. Accedido 15-04-2012).

9.2. Enlaces de interés

- Portal ISO 27000 en español: http://www.iso27000.es.
- International Organization for Standarization (***ISO***): http://www.iso.org/iso/home.html
- International Register of Certificated Auditors (***IRCA***): http://spain.irca.org/auditorcert.html
- Information Systems Audit and Control Association (***ISACA***): http://www.isaca.org/Certification/CISA-Certified-Information-Systems-Auditor/Pages/default.aspx
- ***SANS*** Institute: www.sans.org/.
- Entidad Nacional de Acreditación (***ENAC***): http://www.enac.es.
- Centro Criptológico Nacional (***CCN***): https://www.ccn.cni/
- Capacidad de Respuesta a Incidentes de Seguridad de la Información (***CCN-CERT***) https://www.ccn-cert.cni.es/.

ANEXOS

Esquema de la norma ISO 27001

4. Sistema de Gestión de la Seguridad de la Información.

4.1. Requisitos generales.

Proceso (4.2) documentado (4.3).

4.2. Creación y gestión.

4.2.1. Creación (*Plan*)

a) Alcance y límites del SGSI.
b) Política del SGSI que incluya:
   1) Orientación general.
   2) Requisitos de la actividad, legales, reglamentarios y contractuales.
   3) Alineada con la estrategia de gestión de riesgos de la organización.
   4) Criterios de estimación de riesgo.
   5) Aprobada por la Dirección.
c) Enfoque de evaluación de riesgos:
   1) Especificar una metodología.
   2) Desarrollar criterios de aceptación del riesgo y los niveles aceptables
d) Identificar riesgos:
   1) Activos y sus propietarios.
   2) Amenazas.
   3) Vulnerabilidades.
   4) Impactos en las dimensiones de confidencialidad, integridad y disponibilidad.
e) Analizar y valorar riesgos.
   1) Evaluar efectos en dimensiones de confidencialidad, integridad y disponibilidad.
   2) Evaluar la probabilidad.
   3) Estimar los niveles de riesgo.
   4) Decidir si asumir o tratar [4.2.1c2)].
f) Opciones para el tratamiento de riesgos: gestionar (controles), asumir [4.2.1c2)], evitar, transferir.
g) Seleccionar objetivos de control y controles. (Anexo A, ISO 27002).
h) Aprobación por la dirección de los riesgos residuales propuestos.
i) Autorización de la Dirección para implementar y operar.
j) Elaborar SOA: Controles seleccionados, implementados y excluidos.

4.2.2. Implementación y operación (*Do*).

a) Formular un plan de tratamiento de riesgos: acciones de la dirección, recursos, responsabilidades y prioridades. (Ver cláusula 5).
b) Ejecutar el plan de tratamiento de riesgos.
c) Implementar los controles (4.2.1 g).
d) Definir cómo medir la eficacia de los controles.
e) Programas de formación y concienciación.
f) Gestionar la operación.
g) Gestionar los recursos del SGSI (5.2).
h) Implementar procedimientos de controles preventivos y correctivos.

4.2.3. Supervisión y revisión del SGSI (*Check*).

a) Procedimientos de supervisión y revisión para:
   1) Detectar errores en los procesos.
   2) Identificar debilidades y fortalezas e incidentes de seguridad.
   3) Determinar la eficacia de actividades delegadas o mediante TI.
   4) Detectar eventos y prevenir incidentes de seguridad.
   5) Determinar la eficacia de las acciones.
b) Revisiones periódicas.
c) Medir la eficacia de los controles.
d) Revisar las evaluaciones de riesgos. Planificado y por cambios internos y externos.
e) Realizar auditorías internas. (Cláusula 6). Planificado.
f) Revisar (Dirección) el SGSI. (Ver cláusula 7)
g) Actualizar planes de seguridad.
h) Registrar acciones e incidencias (Cláusula 4.3.3).

4.2.4. Mantenimiento y mejora (*Act*). (Ver cláusula 8)

a) Implementar las mejoras identificadas.
b) Aplicar las medidas correctivas y preventivas (8.2 y 8.3).
c) Comunicar las acciones y mejoras.
d) Asegurar el cumplimiento de objetivos.

4.3. Requisitos de la documentación.

Decisiones y registros, constatar su eficacia y garantizar su disponibilidad.

4.3.1. Generalidades. Se debe incluir.

a) Declaraciones de política [4.2.1 b)] y objetivos.
b) Alcance del SGSI [4.2.1 a)].
c) Procedimientos y mecanismos de control que soporta el SGSI.
d) Metodología de evaluación de riesgos [4.2.1 c)].
e) Informe de evaluación de riesgos [4.2.1 c), 4.2.1 d), 4.2.1 e), 4.2.1 f) y 4.2.1 g)].
f) Plan de tratamiento de riesgos [4.2.2 b)].
g) Procedimientos de procesos de seguridad y medida de controles [4.2.3 c)].
h) Registros requeridos [4.3.3].
i) Declaración de aplicabilidad [4.2.1 j)].

4.3.2. Control de documentos.

a) Aprobación.
b) Revisión, actualización y reaprobación.
c) Control de cambios y revisión de documentos.
d) Disponibilidad de versiones.
e) Legibles e identificables.
f) Acceso, difusión, almacenamiento y destrucción acordes a procedimientos.
g) Identificación de documentos externos.
h) Control de distribución.
i) Prevención de uso no intencionado.
j) Identificación de documentos obsoletos.

4.3.3. Control de registros.

1. De desarrollo del proceso (4.2) e incidentes de seguridad.
2. Crear y mantener, proteger y controlar.
3. Contemplar legislación, regulación y obligaciones contractuales.
4. Legibles, identificables y recuperables.
5. Documentar e implementar controles para identificar, almacenar, proteger, recuperar, retener y disponer.

5. Responsabilidades de la Dirección

5.1. Compromiso de la Dirección. La dirección debe:

a) Formular la política del SGSI.
b) Velar por el establecimiento de objetivos y planes.
c) Definir roles y responsabilidades.
d) Concienciar a la Organización.
e) Proporcionar recursos (5.2.1).
f) Decidir los criterios y niveles de aceptación de riesgos.
g) Velar por la realización de auditorías internas (cláusula 6).
h) Dirigir las revisiones del SGSI (cláusula 7).

5.2. Gestión de los recursos.

5.2.1. Provisión de recursos para:

a) Establecer, implementar, operar, supervisar, revisar, mantener y mejorar el SGSI.
b) Asegurar coherencia entre los procedimientos de seguridad y los requisitos empresariales.
c) Identificar y cumplir requisitos legales y contractuales.
d) Aplicar los controles.
e) Revisar y reaccionar.
f) Mejorar la eficacia del SGSI.

5.2.2. Concienciación, formación y capacitación.

Formación del personal con competencias.
   a) Determinación de competencias.
   b) Impartir formación | Contratar personal competente.
   c) Evaluar la eficacia de las acciones.
   d) Mantener registros de formación (4.3.3).
Concienciación general.

6. Auditorías internas.

A intervalos planificados para determinar si los objetivos de control, controles, procesos y procedimientos:

a) Cumplen con los requisitos de la Norma, legislación y normativa.
b) Cumplen con los requisitos de seguridad de la información.
c) Se implantan y mantienen.
d) Dan el resultado esperado.

El plan de auditorías debe contemplar:

6. Estado e importancia de los procesos y tareas a auditar.
7. Resultado de auditorías previas.
8. Criterios, alcance, frecuencia y métodos de auditoría.
9. Selección de auditores.

Se debe garantizar la objetividad e imparcialidad. Los auditores no pueden auditar su propio trabajo.

Deberá existir un procedimiento documentado que contenga:

10. Responsabilidades.
11. Requisitos para la planificación y realización de las auditorías.
12. Información de los resultados.
13. Mantenimiento de los registros.

El responsable debe velar por realizar las acciones correctoras oportunas que deberán verificarse y generar los informes correspondientes.

7. Revisión del SGSI por la Dirección.

7.1. Generalidades.

La Dirección debe revisar el SGSI a intervalos planificados, al menos una vez al año. Se deben contemplar oportunidades de mejora y cambios en el SGSI. Deberá documentarse y mantener los registros correspondientes.

7.2. Datos iniciales de la revisión.

a) Resultados de auditorías y revisiones previas.
b) Comentarios de las partes interesadas.
c) Técnicas productos o procedimientos que podrían emplearse.
d) Estados de las acciones preventivas o correctivas.
e) Vulnerabilidades o amenazas no abordadas adecuadamente.
f) Resultados de las medidas de eficacia.
g) Acciones de seguimiento.
h) Cambios que afecten al SGSI.
i) Recomendaciones de mejora.

7.3. Resultados de la revisión.

Decisiones y acciones relativas a:

a) Mejora del SGSI.
b) Actualización de evaluación de riesgos y del plan de tratamiento.
c) Modificación de procedimientos y controles, incluyendo cambios en:
   1) Requisitos del negocio.
   2) Requisitos de seguridad.
   3) Procesos de negocio.
   4) Requisitos legales.
   5) Obligaciones contractuales.
   6) Niveles | criterios de aceptación del riesgo.
d) Necesidades de recursos.
e) Cambios en la medida de eficacia de los controles.

8. Mejora del SGSI.

8.1. Mejora continua.

8.2. Acción correctiva / 8.3 Acción preventiva

Procedimientos documentados para:

a) Identificar [posibles] no conformidades.
b) Determinar las causas de las [posibles] no conformidades.
c) Evaluar la necesidad de acciones para evitar | prevenir no conformidades.
d) Determinar e implantar las acciones correctivas | preventivas necesarias.
e) Registrar los resultados de las acciones realizadas | adoptadas.
f) Revisar las acciones correctivas | preventivas adoptadas.

Solo para acciones preventivas:

14. Identificar implicaciones de cambios en los riesgos.
15. Priorizar las acciones preventivas a partir de la evaluación de riesgos.

ISO 27001 Anexo A (ISO 27002). Código de buenas prácticas para la gestión de la seguridad de la información. (Dominios, Objetivos de control y controles).

5. Política de Seguridad.
5.1. Política de seguridad de la información.
5.1.1. Documento de política de seguridad de la información.
5.1.2. Revisión de la política de seguridad de la información.

6. Aspectos Organizativos.
6.1. Organización interna.
6.1.1. Comité de gestión de seguridad de la información.
6.1.2. Coordinación de la seguridad de la información.
6.1.3. Asignación de responsabilidades de la seguridad de la información.
6.1.4. Proceso de autorización de recursos para proceso de información.
6.1.5. Acuerdos de confidencialidad.
6.1.6. Contacto con las autoridades.
6.1.7. Contacto con grupos de especial interés.
6.1.8. Revisión independiente de la seguridad de la información.
6.2. Terceros.
6.2.1. Identificación de los riesgos derivados del acceso de terceros.
6.2.2. Tratamiento de seguridad en la relación con los clientes.
6.2.3. Tratamiento de seguridad en contratos con terceros (*outsourcing*).

7. Gestión de activos.
7.1. Responsabilidad sobre los activos.
7.1.1. Inventario de activos.
7.1.2. Propiedad de los activos.
7.1.3. Uso aceptable de los activos.
7.2. Clasificación de la información.
7.2.1. Directrices de clasificación.
7.2.2. Etiquetado y manipulado de la información.

8. Seguridad ligada a los recursos humanos.
8.1. Antes del empleo.
8.1.1. Funciones y responsabilidades.
8.1.2. Investigación de antecedentes.
8.1.3. Términos y condiciones de contratación.
8.2. Durante el empleo.
8.2.1. Responsabilidades de la Dirección.
8.2.2. Concienciación, formación y capacitación en seguridad de la inform.
8.2.3. Proceso disciplinario.
8.3. Cese del empleo o cambio de puesto de trabajo.
8.3.1. Responsabilidad en el cese o cambio.
8.3.2. Devolución de activos.
8.3.3. Retirada de los derechos de acceso.

9. Seguridad física y ambiental.
9.1. Áreas seguras.
9.1.1. Perímetro de seguridad física.
9.1.2. Controles físicos de entrada.
9.1.3. Seguridad de oficinas, despachos e instalaciones.
9.1.4. Protección contra las amenazas externas y de origen ambiental.
9.1.5. Trabajo en áreas seguras.
9.1.6. Áreas de acceso público y de carga y descarga.
9.2. Seguridad de los equipos.
9.2.1. Emplazamiento y protección de equipos.
9.2.2. Instalaciones de suministro.
9.2.3. Seguridad del cableado.
9.2.4. Mantenimiento de los equipos.
9.2.5. Seguridad de los equipos fuera de las instalaciones.
9.2.6. Reutilización o retirada segura de equipos.
9.2.7. Retirada de materiales propiedad de la empresa.

10. Gestión de comunicaciones y operaciones.
10.1. Responsabilidades y procedimientos de operación.
10.1.1. Documentación de los procedimientos de operación.
10.1.2. Gestión de cambios.
10.1.3. Segregación de tareas.
10.1.4. Separación de entornos de desarrollo, prueba y operación.
10.2. Gestión de la provisión de servicios por terceros.
10.2.1. Provisión de servicios.
10.2.2. Supervisión y revisión de los servicios prestados por terceros.
10.2.3. Gestión de cambios en los servicios prestados por terceros.
10.3. Planificación y aceptación del sistema.
10.3.1. Gestión de capacidades.
10.3.2. Aceptación del sistema.
10.4. Protección contra código malicioso y descargable.
10.4.1. Controles contra el código malicioso.
10.4.2. Controles contra el código descargado en el cliente.
10.5. Copias de seguridad.
10.5.1. Copias de seguridad de la información.
10.6. Gestión de la seguridad de las redes.
10.6.1. Controles de red.
10.6.2. Seguridad de los servicios de red.
10.7. Manipulación de los soportes.
10.7.1. Gestión de soportes extraíbles.
10.7.2. Retirada de soportes.
10.7.3. Procedimientos de manipulación de la información.
10.7.4. Seguridad de la documentación del sistema.
10.8. Intercambio de información.
10.8.1. Políticas y procedimientos de intercambio de información.
10.8.2. Acuerdos de intercambio.
10.8.3. Soportes físicos en tránsito.
10.8.4. Mensajería electrónica.
10.8.5. Sistemas de información empresariales.
10.9. Servicios de comercio electrónico.
10.9.1. Comercio electrónico.
10.9.2. Transacciones en línea.
10.9.3. Información puesta a disposición pública.
10.10. Supervisión.
10.10.1.Registro de auditorías.
10.10.2.Supervisión del uso del sistema.
10.10.3.Protección de la información de los registros..
10.10.4.Registros de administración y operación.
10.10.5.Registro de fallos.
10.10.6.Sincronización del reloj.

11. Control de acceso.
11.1. Requisitos de negocio para el control de acceso.
11.1.1. Política de control de acceso.
11.2. Gestión de acceso de usuario.
11.2.1. Registro de usuario.
11.2.2. Gestión de privilegios.
11.2.3. Gestión de contraseñas de usuario.
11.2.4. Revisión de los derechos de acceso de usuario.
11.3. Responsabilidades de usuario.
11.3.1. Uso de contraseña.
11.3.2. Equipo de usuario desatendido.
11.3.3. Política de puesto de trabajo y pantalla limpia.
11.4. Control de acceso a la red.
11.4.1. Política de uso de los servicios en red.
11.4.2. Autenticación de usuario para conexiones externas.
11.4.3. Identificación de los equipos en las redes.
11.4.4. Diagnóstico remoto y protección de los puertos de configuración.
11.4.5. Segregación de las redes.
11.4.6. Control de conexión a la red.
11.4.7. Control de encaminamiento (*routing*) de red.
11.5. Control de acceso al sistema operativo.
11.5.1. Procedimientos seguros de inicio de sesión.
11.5.2. Identificación y autenticación de usuario.
11.5.3. Sistema de gestión de contraseñas.
11.5.4. Uso de los recursos del sistema.
11.5.5. Desconexión automática de sesión.
11.5.6. Limitación del tiempo de conexión.
11.6. Control de acceso a las aplicaciones y a la información.
11.6.1. Restricción del acceso a la información.
11.6.2. Aislamiento de sistemas sensibles.
11.7. Ordenadores portátiles y teletrabajo.
11.7.1. Ordenadores portátiles y comunicaciones móviles.
11.7.2. Teletrabajo.

12. Adquisición, desarrollo y mantenimiento de los sistemas de información.
12.1. Requisitos de seguridad de los sistemas de información.
12.1.1. Análisis y especificación de los requisitos de seguridad.
12.2. Tratamiento correcto de las aplicaciones.
12.2.1. Validación de datos de entrada.
12.2.2. Control del procesamiento interno.
12.2.3. Integridad de los mensajes.
12.2.4. Validación de los datos de salida.
12.3. Controles criptográficos.
12.3.1. Política de uso de los controles criptográficos.
12.3.2. Gestión de claves.
12.4. Seguridad de los archivos de sistema.
12.4.1. Control del software en explotación.
12.4.2. Protección de los datos de prueba del sistema.
12.4.3. Control de acceso al código fuente de los programas.
12.5. Seguridad en los procesos de desarrollo y soporte.
12.5.1. Procedimientos de control de cambios.
12.5.2. Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.
12.5.3. Restricciones a los cambios en los paquetes de software.
12.5.4. Fugas de información.
12.5.5. Externalización (*outsourcing*) del desarrollo del software.
12.6. Gestión de la vulnerabilidad técnica.
12.6.1. Control de las vulnerabilidades técnicas.

13. Gestión de incidentes de seguridad de la información.
13.1. Notificación de eventos y puntos débiles de la seguridad de la información.
13.1.1. Notificación de los eventos de seguridad de la información..
13.1.2. Notificación de los puntos débiles de la seguridad.
13.2. Gestión de incidentes de la seguridad de la información y mejoras.
13.2.1. Responsabilidades y procedimientos.
13.2.2. Aprendizaje de los incidentes de seguridad de la información.
13.2.3. Recopilación de evidencias.

14. Gestión de continuidad del negocio.
14.1. Aspectos de seguridad en la gestión de la continuidad del negocio.
14.1.1. Inclusión de la seguridad de la información en el proceso de gestión del la continuidad del negocio.
14.1.2. Continuidad del negocio y evaluación de riesgos.
14.1.3. Desarrollo e implantación de planes de continuidad que incluyan la seguridad de la información.
14.1.4. Marco de referencia para la planificación de la continuidad del negocio.
14.1.5. Pruebas, mantenimiento y reevaluación de los planes de continuidad del negocio.

15. Cumplimiento.
15.1. Cumplimiento de los requisitos legales.
15.1.1. Identificación de la legislación aplicable.
15.1.2. Derechos de propiedad intelectual (DPI/*IPR*).
15.1.3. Protección de los documentos de la Organización.
15.1.4. Protección de datos y privacidad de la información personal.
15.1.5. Prevención del uso indebido de los recursos de tratamiento de la información.
15.1.6. Regulación de los controles criptográficos.
15.2. Cumplimiento de las políticas y normas de seguridad y reglamentos técnicos
15.2.1. Cumplimiento de las políticas y normas de seguridad.
15.2.2. Comprobación del cumplimiento de reglamentos técnicos.
15.3. Consideraciones sobre la auditoría de los sistemas de información.
15.3.1. Controles de auditoría de los sistemas de información.
15.3.2. Protección de las herramientas de auditoría de los sistemas de información.