

IS2ME

Seguridad de la Información a la Mediana Empresa

Un Método para Acercar e Implementar la Seguridad de la Información en las Pequeñas y Medianas Empresas

Autores:

Samuel Linares (Samuel.Linares@tecnocom.es)

Ignacio Paredes (Ignacio.Paredes@tecnocom.es)

IS2ME: Seguridad de la Información a la Mediana Empresa (Information Security to Medium Enterprise)

Un método para acercar e implementar la seguridad de la información en las pequeñas y medianas empresas

1 Introducción/Antecedentes

Los términos PYME (Pequeñas y Medianas Empresas) o SME (Small and Medium Enterprises) representan un concepto muy difundido en todo el mundo para hacer referencia a un tipo de empresa con un número reducido de trabajadores y cuya facturación es moderada, factores estos determinantes para identificar una organización de este tipo. Teniendo en cuenta estos parámetros, existen diferentes criterios dependiendo de cuál sea el país elegido, por lo que en este documento se identificarán como medianas empresas aquellas organizaciones con un número de empleados inferior a 500 (aproximadamente) lo que, de forma general, engloba a más del 90% del total de las empresas existentes en el mundo y a más del 99% de las existentes en la Unión Europea.

Los profesionales de la seguridad de la información habitualmente involucrados en temas como el gobierno y la gestión de la seguridad de la información, sus métricas, estándares, proyectos de firma digital e infraestructuras de clave pública o consolidación de registros, entre otros, sufren cierta pérdida de perspectiva al asumir como cierto y existente el conocimiento, implantación y la cultura en seguridad de la información en las empresas en general, cuando la situación real, en el caso de las medianas empresas, es otra. Un pequeño número de empresas tienen unos niveles muy altos de implantación de seguridad de la información mientras que la gran mayoría tiene carencias importantes en el conocimiento de la seguridad en general, y en la implantación de las medidas técnicas y organizativas asociadas, en particular, existiendo una clara falta de madurez en las organizaciones de este tipo en lo que a seguridad de la información se refiere.

Habitualmente no existe en estas empresas una estructura organizativa adecuada, careciendo en muchos casos de la figura del responsable de seguridad, cuyo rol asume la misma persona responsable de IT (sistemas y/o comunicaciones), lo que unido a la falta de responsabilidad explícita y a las importantes carencias formativas en el área de seguridad de la información, hace que las medidas de seguridad implantadas suelen ser muy básicas y respondan en casi todos los casos, a necesidades puntuales para solventar un problema existente, o a la implantación de una nueva funcionalidad o aplicación dentro de la organización.

La labor diaria, el “día a día”, no permite a sus responsables tomar una visión de conjunto o realizar una planificación y gestión adecuada de la seguridad, lo que a su vez se traduce en una falta de concienciación de la alta dirección en estos temas y por ende, en la asunción de unos niveles de riesgo inaceptables para la organización que desafortunadamente, suelen materializarse en el momento de la ocurrencia de un incidente de seguridad o de la necesidad de cumplimiento de una ley o norma, que habitualmente tiene asociado un importante impacto en el negocio. Es en ese momento de forma inmediata, o de forma más planificada si la organización cuenta con una mente preclara que logre impulsar una iniciativa previa en ese sentido, cuando se requiere la presencia de los profesionales de la seguridad de la información para, por una parte solucionar los problemas existentes en esa materia, y por otra comenzar el camino hacia la disminución del riesgo y la implantación de las medidas de seguridad adecuadas.

Suelen ser requisitos indispensables marcados por la compañía en estos casos, la pronta disponibilidad de resultados que disminuyan el riesgo existente, la implantación de medidas de seguridad críticas a corto plazo y con total certeza, la presentación de un plan de acción que permita tanto a la alta dirección como al actual responsable de seguridad (camuflado como responsable de tecnologías de la información) identificar qué recursos serán necesarios y cuál será el camino que deban seguir para incorporar la seguridad como un requisito más en sus procesos de negocio.

Ante tamaño reto, el profesional de la seguridad de la información siempre podrá abordarlo mediante un enfoque tradicional siguiendo las metodologías y estándares existentes (ISO 27001 principalmente) y por tanto comenzar con el proceso de implantación del SGSI (Sistema de Gestión de la Seguridad de la Información) mediante las consabidas fases, cuya descripción no es objeto de este documento, pero que como referencia se mencionan a continuación:

- Definición de la política y alcance del SGSI
- Establecimiento de Responsabilidades y Recursos
- Registro de activos
- Gestión del riesgo
- Selección de controles aplicables
- Establecimiento de aplicabilidad
- Implantación

El seguimiento estricto de estas fases en este tipo de empresas suele ser muy complicado debido a la falta de concienciación de la alta dirección y a la inexistencia del entorno inicial sobre unas bases mínimas en lo que a seguridad de la información se refiere. La implantación de medidas de seguridad (controles) no comienza hasta bien avanzado el proyecto (varios meses después probablemente) y por tanto, uno de los fines (justificado, al fin y al cabo) perseguidos por la compañía, la implantación de medidas de seguridad críticas a corto plazo, no es tenido en cuenta inicialmente.

Este enfoque, acertado y completo por otra parte, no suele ser aceptado generalmente, ya que se buscan unos resultados más “inmediatos” y prácticos a corto plazo (“*queremos seguridad, y la queremos ahora*”), si bien sí que se acepta como el camino a seguir a medio o largo plazo.

Es aquí donde surge la necesidad de una metodología o aproximación que ante escenarios como el mencionado (no debe olvidarse que las empresas que estamos tratando suponen un 99% de las existentes en la Unión Europea), ofrezca una alternativa puente entre el incumplimiento total y la implantación metodológica de la gestión de la seguridad mediante un estándar como ISO 27001.

En este sentido se presenta IS2ME, Information Security to the Medium Enterprise (Seguridad de la Información a la Mediana Empresa) como solución y aproximación para el camino a seguir hacia la implementación de la seguridad de la información en empresas cuyo modelo de seguridad aún no es maduro y desean acometer la labor de implantación de la seguridad de la información y de su sistema de gestión asociado de una forma eficiente, eficaz y práctica, de forma que permita disminuir el riesgo de la organización a corto plazo a la vez que se inicie el camino hacia el cumplimiento de los estándares deseados.

IS2ME persigue también un objetivo social ambicioso: el acercamiento de la seguridad de la información a las medianas (y pequeñas) empresas, fomentando así su penetración en la cultura organizacional del tejido empresarial existente y disminuyendo en general el nivel de riesgo asumido por las organizaciones, aumentando con ello su valor y rentabilidad y elevando, por tanto, el nivel económico de la mayoría de las empresas existentes en la actualidad.

2 Objetivos

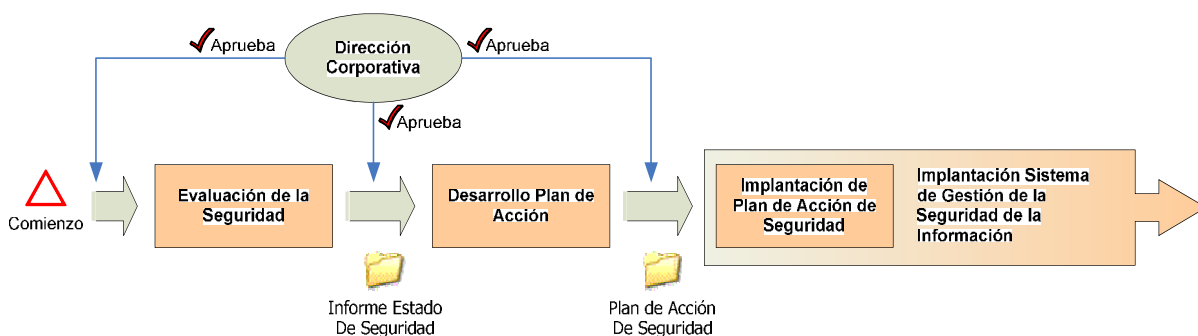
El método IS2ME tiene como uno de sus principales objetivos la disminución urgente del riesgo asumido por la organización en lo que a Seguridad de la Información se refiere. Mediante el establecimiento de un entorno o marco de implantación de las medidas técnicas y organizativas necesarias, se desarrollarán unas fases de implantación que permitan la elaboración de un proyecto asociado cuyo fin último será la incorporación de la seguridad de la información en la cultura organizacional como un requisito más del negocio, obteniendo a su vez resultados parciales a corto plazo que identifiquen el estado actual de la seguridad de la organización, las acciones necesarias para su mejora y el plan de acción para la implementación de esas acciones.

Para el desarrollo de estas fases se incorporará como requisito ineludible a las mismas el cumplimiento implícito de los estándares o normas que en cada acción puedan ser aplicables. No se pretende aquí desarrollar un nuevo estándar de gestión de la seguridad de la información (y por tanto “la reinención de la rueda”), sino proponer un método claro y definido de acercamiento de las pequeñas y medianas empresas al cumplimiento de los estándares deseados, mediante la ejecución de unas fases con objetivos claros que puedan ser fácilmente evaluables por la organización y que aporten beneficios y resultados inmediatos en la mejora de los niveles de implantación de la seguridad en la misma, sentando así la base para su posterior desarrollo en profundidad hacia el cumplimiento e implantación total del Sistema de Gestión de la Seguridad de la Información según las normas existentes, si así se desea.

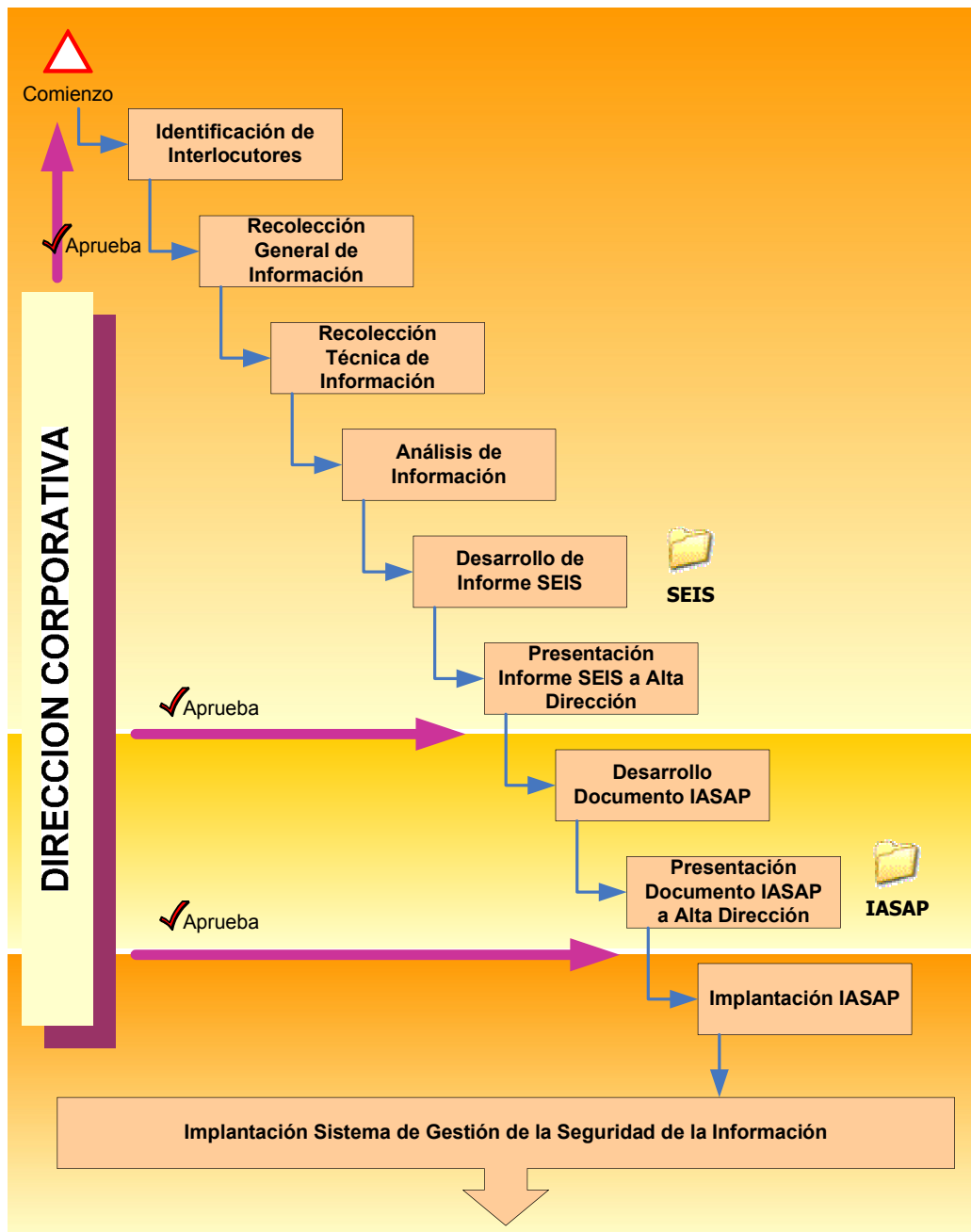
Una de las bases para conseguir los objetivos mencionados será no sólo considerar la seguridad como algo abstracto y general, sino evaluar, y por tanto analizar y proponer en detalle, las medidas técnicas y organizativas correspondientes. Aspectos organizativos como la estructura de la organización, roles existentes, responsabilidades definidas o flujos de información, entre otros, serán estudiados a la vez que otros más técnicos como arquitectura y topología de servicios, redes, sistemas y comunicaciones, dispositivos de seguridad existentes o análisis de vulnerabilidades, etc.

3 El Método

De forma general, IS2ME comienza evaluando la seguridad de la organización mediante la recolección de información a través de entrevistas con personal de la organización, realización de pruebas de campo y análisis técnicos, para a continuación, presentado un informe del estado de implantación de las distintas medidas de seguridad técnicas y organizativas, pasar a la elaboración y propuesta de un plan de acción que, tras ser aprobado por la alta dirección, se procederá a su desarrollo e implementación, sentando la base y comenzando el camino hacia el cumplimiento e implantación del Sistema de Gestión de la Seguridad de la Información según ISO 27001.



En la elaboración de IS2ME se ha pretendido seguir un enfoque holístico y extremadamente práctico que permita al usuario del mismo una aplicación sencilla e inmediata mediante el seguimiento de unas fases secuenciales bien diferenciadas que son mostradas en la siguiente figura y se describen en detalle a continuación.



3.1 Identificación de Interlocutores

Objetivo: Identificación de interlocutor (o interlocutores) válidos en la organización y planificación de su disponibilidad por parte de la organización.

La fase de recolección de información tiene una gran importancia en el desarrollo del método puesto que la información obtenida en la misma será la fuente del análisis y desarrollo del estado en seguridad de la información de la organización y del posterior plan de acción. Por ello, para el desarrollo de esa fase deberá contarse con la colaboración total de la organización para la obtención de la información correspondiente.

Habitualmente la organización deberá nombrar una persona (o varias de ser necesario) que ejercerá como interlocutor entre el equipo de trabajo que esté desarrollando el estudio y la organización, de forma que se realizarán las correspondientes consultas al interlocutor y éste las trasladará a las personas que corresponda dentro de la organización. Será importante que la organización prevea su disponibilidad durante el periodo de recolección de datos.

Adicionalmente, para determinadas tareas que serán claramente identificadas previamente por el equipo de trabajo, podrá ser necesario el acceso directo a determinados dispositivos y sistemas de la compañía para realizar comprobaciones de configuración, de seguridad, etc. Este acceso deberá ser proporcionado por la organización con los requisitos que ésta estime oportunos: bajo supervisión de personal propio, con diario de operaciones efectuadas, o cualquier mecanismo que ofrezca unas funcionalidades similares y salvaguarde la integridad de la información. El equipo de trabajo firmará un acuerdo de confidencialidad constituyendo una garantía hacia la organización de no difusión ni utilización de la información tratada. Así mismo la organización deberá firmar por escrito una autorización para realizar las pruebas que el equipo de trabajo indique y estime oportunas para obtener la información necesaria para la realización de las tareas encomendadas.

3.2 Recolección General de Información

Objetivo: Obtención de todo tipo de información mediante entrevistas, revisión de documentación y métodos análogos referente a seguridad de la información, que deberá incluir información técnica, organizativa y de cumplimiento.

Como ya se comentó anteriormente, teniendo en cuenta que la información recolectada en esta fase será la que servirá como base para el desarrollo completo del proceso de análisis y elaboración del plan de acción, esta será una de las fases clave en el desarrollo de IS2ME, por lo que se deberá prestar especial interés en la consecución del objetivo marcado.

En esta fase inicial se recolectará la información necesaria de la compañía que supondrá el origen de las posteriores baterías de pruebas y análisis técnicos necesarios. Durante esta fase se tendrá una mayor interacción entre la organización y el equipo de trabajo que se verá materializada por la presencia local del mismo en la localización de la organización, redundando todo esto en un diálogo fluido y efectivo que facilitará la obtención de la información deseada. Deberá por tanto proporcionarse el espacio y tiempo disponible del interlocutor para su realización.

De forma previa a la presencia del equipo de trabajo en la organización, podrá facilitarse al interlocutor seleccionado un cuestionario que, en su caso, deberá ser remitido adecuadamente cubierto al equipo de trabajo para llevar a cabo la recolección de información de la forma más eficiente posteriormente. Este formulario podrá contener cuestiones técnicas y organizativas sobre la organización, departamento o área objeto del estudio que permitirán al equipo de trabajo focalizar el esfuerzo durante su estancia en sus instalaciones, de forma que se maximice el resultado y minimice el tiempo

empleado, tanto por la organización como por el equipo de trabajo, en la labor de recolección de información.

Deberá obtenerse, al menos, la siguiente información:

- Aspectos Técnicos:
 - o Topología y arquitectura de red y servicios existente y descripción de la misma
 - o Servicios ofrecidos al público e internamente y a través de qué medio (Internet, redes privadas virtuales, etc.)
 - o Elementos/Dispositivos de seguridad existentes en la red y breve descripción funcional (firewalls, IDSs, IPSs, sistemas antivirus centralizados/distribuidos, proxies, etc.)
 - o Existencia de posibles puntos de interconexión con otras redes, descripción de las posibles DMZs existentes, niveles de seguridad, etc.
 - o Posibles puntos de fallo conocidos de la red, dispositivos, servidores, etc. Mecanismos de alta disponibilidad existentes. Procedimientos de emergencia asociados, responsables, etc.
 - o Plan de direccionamiento de la red (público y privado) y procedimientos asociados al mismo (asignación de direcciones, solicitud, etc.)
 - o Documentación existente relativa a la red, servicios, etc. Procedimientos asociados a la misma.
 - o Existencia de gestión de red y servicios, descripción de la misma y procedimientos asociados.

- Aspectos Organizativos y de Cumplimiento:
 - o Definición de la organización, áreas o departamentos objeto del estudio (a qué se dedica, cuáles son sus funciones, de qué es responsable, etc.).
 - o Estructura organizativa de la compañía aplicable al estudio, dentro de su alcance. Relaciones con otras áreas, departamentos u organizaciones. Roles existentes, flujos, responsables, etc.
 - o Enumeración y descripción de las políticas, procedimientos, instrucciones de trabajo o normas existentes en la compañía que son susceptibles de cumplimiento (ISO9001, políticas de seguridad, políticas de comunicación, políticas de uso de recursos, etc.)
 - o Enumeración y explicación de otras políticas de seguridad o documentos existentes que puedan ser de aplicación.
 - o Enumeración y descripción del cumplimiento actual en legislación de las tecnologías de la información aplicable.

3.3 Recolección Técnica de Información

Objetivo: Obtención de todo tipo de información mediante diversos métodos técnicos y empíricos en una muestra representativa de los sistemas y dispositivos de la organización.

Partiendo de la información recolectada en la fase anterior, se procederá a identificar los sistemas objeto de estudio para a continuación realizar una serie de análisis técnicos con el fin de conocer de forma precisa cuál es su estado real desde un punto de vista de seguridad técnica. Mediante estos análisis seremos capaces de detectar problemas de seguridad, existentes o potenciales, que puedan afectar a la integridad de los sistemas de la organización, además de a su funcionamiento o rendimiento.

A continuación se enumeran los distintos puntos que deberán ser abordados durante la recolección técnica de información.

3.3.1 Enumeración y Caracterización

Tomando como base la información general recopilada en la fase “Recolección General de Información”, se identificarán los sistemas, dispositivos y aplicaciones sobre los que se realizará el estudio técnico, llevando a cabo una caracterización lo más exhaustiva posible de cada elemento puesto que esta información resultará de mucha utilidad a la hora de realizar los análisis técnicos y la interpretación de los resultados.

La información mínima que deberá recopilarse será la siguiente (aunque podrá ser ampliada con aquellos datos que el equipo de trabajo pueda considerar de interés):

Caracterización de Sistemas

- Sistema (nombre, tipo, fabricante)
- Ubicación
- Responsable
- Versiones software (SSOO, aplicaciones que corren en él)
- Estado de parches y/o actualizaciones

Caracterización de Aplicaciones

- Aplicación (nombre, fabricante, versión)
- Subsistemas asociados (sistemas en que corre)
- Interrelación con otras aplicaciones
- Responsable
- Estado de parches y/o actualizaciones

3.3.2 Análisis de Tráfico

Mediante el análisis de tráfico se intentará caracterizar el tipo de tráfico que discurre habitualmente por las redes de la organización, así como detectar posibles puntos de fallo o cuellos de botella en dichas redes.

Para un óptimo resultado del análisis, deberán identificarse cuáles son los puntos *sensibles* en los que deberán realizarse las medidas, entendiendo por *sensibles* aquellos puntos con representatividad en su tráfico. Dichos puntos, típicamente podrán ser:

- Interconexiones entre segmentos
- Segmentos de servidores/aplicaciones críticas
- Segmentos de usuarios
- Otros puntos de interés

Cada medida deberá realizarse durante un periodo de tiempo significativo de forma que se capture una cantidad de tráfico suficiente para su posterior análisis. El tiempo de medida dependerá de la cantidad de tráfico que habitualmente soporta la red. En algunos entornos será suficiente mantener la medida durante unos pocos minutos, mientras que en otros será necesario realizar la medida a lo largo de un día completo o incluso, periodos más prolongados de tiempo.

También será necesario tener en cuenta las franjas temporales de utilización de la red. Por ejemplo, no será lo mismo la captura de tráfico en una red de oficina, que en una red de una fábrica en la que se realizan trabajos 24 horas al día. Por tanto, será importante conocer las pautas de utilización de la red con el fin de seleccionar los momentos de medida adecuados.

Las capturas, por norma general, se realizarán sin ningún tipo de filtrado, y se almacenarán en disco de forma que puedan ser reproducidas y tratadas en laboratorio con el fin de generar informes y estadísticas de uso. Para su realización se utilizará cualquier analizador de protocolos que permita la realización de las tareas anteriormente comentadas.

3.3.3 Análisis de Vulnerabilidades Sistemas y Aplicaciones

El análisis de vulnerabilidades de sistemas y aplicaciones tiene como objeto detectar puntos débiles en la seguridad de los sistemas y aplicaciones que éstos soportan. Entendemos por puntos débiles, errores de programación o de configuración en las aplicaciones y sistemas operativos que puedan ser causa de vulnerabilidades susceptibles de ser explotadas por potenciales atacantes. Por tanto, será importante conocer cuáles son estos puntos débiles con el fin de implantar los controles adecuados para eliminarlos o evitar su explotación.

No todos los sistemas tienen la misma importancia dentro de la organización. Por esto, y porque el análisis de vulnerabilidades es una tarea que puede consumir mucho tiempo, deberá realizarse una selección de cuáles son los sistemas sobre los que se realizará el análisis. Objetivos típicos de este tipo de análisis serán los sistemas cuyo mal funcionamiento pueda causar un impacto importante en los procesos de la organización (e.g. Servidores principales) o aquellos que por su visibilidad están más expuestos a posibles ataques (e.g. Servidores con acceso público desde Internet). Deberá ser la organización objeto del análisis quien, con el asesoramiento del equipo de trabajo que efectúe el análisis, decida cuáles son los sistemas que deben ser analizados.

3.3.3.1 Análisis remoto

Se prestará especial atención a las vulnerabilidades que pueden ser explotadas remotamente, ya que éstas pueden suponer un mayor riesgo al no requerir de presencia física para su explotación. Dichas vulnerabilidades, habitualmente estarán asociadas a puertos de aplicación que esperan recibir conexiones remotas. El primer paso del análisis de vulnerabilidades, por tanto, será identificar cuáles son los puertos de los sistemas que son accesibles de forma remota. Un método para conseguir esta información será la realización de un escaneo de puertos.

El objetivo del escaneo de puertos será averiguar qué puertos (típicamente TCP o UDP) están a la escucha en un sistema determinado, y por tanto, pueden recibir conexiones remotas. Es esta una información de suma importancia, ya que una gran parte de las vulnerabilidades asociadas a aplicaciones, tienen que ver con las posibilidades de conexión remota de las mismas. La técnica básica para saber el estado de un puerto es tratar de realizar una conexión contra el mismo y analizar el resultado, pudiendo obtenerse tres valores para el estado de un puerto:

- Abierto: El puerto está a la escucha y listo para recibir conexiones.
- Cerrado: El puerto no está a la escucha
- Filtrado: Existe algún dispositivo (típicamente un cortafuegos/firewall) que no permite realizar conexiones contra el puerto

Existen diferentes técnicas de escaneo de puertos, muchas de ellas orientadas a tratar de evitar métodos de detección y seguridad de los sistemas objetivo, pero en el caso que nos ocupa pueden no ser relevantes, ya que deberá contarse con la aprobación y el permiso por escrito del propietario de los sistemas para realizar el escaneo y las acciones correspondientes, pudiendo realizar los escaneos y análisis sin necesidad de utilizar técnicas de camuflaje (*stealth*), salvo en el caso en que existan dispositivos de seguridad (como sistemas de prevención de intrusiones) que puedan invalidar los resultados de dichas pruebas.

Una vez establecido el alcance de los sistemas sobre los que se realizará el análisis, se deberá elegir la profundidad del mismo, es decir, deberá decidirse sobre qué puertos se realizarán las posteriores comprobaciones. Evidentemente, para que el análisis sea completo, debería comprobarse el estado de todos los puertos (tanto TCP como UDP¹), pero dado que en ocasiones esto puede llevar más tiempo del que se tendrá disponible, en ciertos casos será posible reducir el número de puertos a analizar, bien porque se tenga la certeza de que el sistema sólo escucha en ciertos puertos, o porque existan dispositivos de filtrado que sólo permitan la conexión a puertos determinados. De esta forma, la complejidad del escaneo de puertos y el consiguiente análisis de vulnerabilidades se reducirá haciéndose mucho más manejable.

Tras realizar el escaneo de puertos, dispondremos de la información referente a qué puertos tiene disponibles cada sistema para aceptar conexiones remotas. Cada uno de estos puertos estará asociado a un servicio y por tanto a una aplicación. El siguiente paso será averiguar cuáles son dichas aplicaciones y, si es posible, la versión de las mismas.

Conocer el software específico que está instalado en un sistema es una de las primeras labores que intentará abordar un potencial atacante, ya que con esta información, se pueden conocer cuáles son las vulnerabilidades que presentan las aplicaciones remotamente accesibles, y de esta forma acceder a los métodos de explotación de la vulnerabilidad (o *exploits*). El resultado de la ejecución de un *exploit* se materializa habitualmente en un compromiso del sistema, que puede ir desde la eventual destrucción de sus datos al acceso no lícito de sus recursos.

La identificación de software a partir de los puertos por los que escucha puede realizarse mediante las respuestas (*banners*) que proporciona el servicio ante una conexión entrante. No obstante, dado que los *banners* pueden (y deben) ser modificados por motivos de seguridad, esta no es una manera adecuada de realizar esta tarea. Existen multitud de aplicaciones, muchas de ellas de código libre (*open source*), que automatizan la tarea de identificar las aplicaciones asociadas a un puerto. Estas aplicaciones no se limitan a reconocer los *banners* de respuesta, sino que analizan las respuestas de la aplicación ante ciertas entradas, y en base a diferencias de implementación conocidas, son capaces de deducir, eso sí, con un grado de precisión variable, la aplicación y versión que está proporcionando el servicio en cuestión.

Este proceso (escaneo + identificación), es la forma en la que un posible atacante trabajaría, y es importante llevarlo a cabo con el fin de crear consciencia de qué información podría ser obtenida con estos medios. No obstante, desde el punto de vista del análisis de seguridad, y con el fin de tener certeza sobre la veracidad de los resultados obtenidos, la identificación de aplicaciones y sus versiones debería ser abordada adicionalmente mediante el análisis local de los sistemas en cuestión.

En este punto, a un posible atacante le bastaría consultar alguno de los múltiples servicios disponibles en Internet que permiten conocer las vulnerabilidades (y los *exploits*) de una versión de aplicativo determinada. Por el contrario, la labor del equipo de trabajo será averiguar cuáles son los parches o actualizaciones adecuadas para solucionar los problemas de dicho aplicativo. En caso de que no existiesen o no se pudiesen aplicar dichos parches o actualizaciones, deberán buscarse alternativas que disminuyan el nivel de riesgo de exposición de estas aplicaciones.

Actualmente, las redes de comunicaciones en las que se ubican los sistemas analizados, son rara vez planas. Es habitual la existencia de diferentes segmentos, separados por diferentes dispositivos y con distintas políticas de acceso. Por tanto, el análisis de vulnerabilidades ofrecerá diferentes resultados dependiendo desde qué origen se realice. Teniendo esto en cuenta, para que los resultados de los análisis sean válidos, éstos deberán ser realizados desde todas las posibles ubicaciones que puedan

¹ En este documento se hace referencia únicamente a redes de comunicaciones IP por corresponder a la gran mayoría de las existentes en este tipo de organizaciones. Si la red de la organización analizada estuviese soportada por otro protocolo, debería actuarse de forma análoga con las particularidades aplicables a dicho protocolo

ocupar los potenciales atacantes, ofreciendo así distintos perfiles de visibilidad (y de exposición al riesgo) del sistema analizado.

De forma típica, se realizarán análisis desde las siguientes ubicaciones:

- **Internet:** Desde Internet se tendrá acceso a los servicios públicamente accesibles de la organización. Mediante este análisis se verificará que sólo estos servicios son accesibles de forma pública.
- **DMZ:** Si en la organización existen segmentos de DMZ, deberán realizarse los escaneos hacia los servidores internos desde esta ubicación, ya que es un punto de entrada habitual una vez que ha sido comprometido alguno de los servidores públicos. De esta forma podrá conocerse qué grado de visibilidad tendrán los servidores internos para un atacante que ya ha conseguido comprometer algún sistema de la organización.
- **Mismo segmento:** El escaneo desde el mismo segmento de red permite conocer sin acceder físicamente al sistema cuáles son los servicios que tiene configurados, tanto los que se están utilizando como los que están en funcionamiento sin ser utilizados debido a malas prácticas de administración o instalaciones por defecto.
- **Red Interna:** Dado que una gran parte de los incidentes de seguridad en los sistemas de las organizaciones proviene de la propia organización, es importante conocer qué servicios son accesibles (y por tanto posibles causas de vulnerabilidad) desde las redes de usuarios internos.

3.3.3.2 Análisis local

Mediante el análisis local pretendemos obtener un conocimiento preciso del estado de seguridad del sistema. Este análisis no suele estar al alcance de los posibles atacantes, pero puede resultar de suma utilidad para conocer el estado del sistema desde el punto de vista de la seguridad. De forma resumida, lo que se trata de conseguir es la caracterización más completa posible del sistema en cuestión.

En este sentido, deberá recolectarse al menos la siguiente información de forma general:

Nombre
Responsable
Tipo de sistema
Sistemas de ficheros
Utilización de Memoria
Parches o Actualizaciones
Software o Aplicativos instalados
Puertos a la escucha y conexiones activas
Banners de servicios
Servicios y Scripts de arranque
Listas de procesos en ejecución
Usuarios y contraseñas
Configuración de red
Tareas de ejecución periódica

Adicionalmente, dependiendo del sistema operativo del dispositivo analizado podrá ser necesaria la recopilación de otros datos que, en ese caso, deberán ser identificados por un experto en esa área. Un ejemplo para sistemas Unix podrían ser la recopilación de Tcp wrappers, Ficheros SUID y SGID, Servicios NFS o Servicios RPC, entre otros.

3.3.4 Revisión de configuraciones

Durante la recolección técnica de información se revisarán también las configuraciones de elementos clave de la red de la organización. Muchas veces, debido al volumen de elementos de red no será posible realizar una revisión exhaustiva, sin embargo, será necesario en este caso decidir de acuerdo con el interlocutor de la organización cuáles serán los dispositivos sobre los que se realizará el análisis.

Para la revisión de las configuraciones será necesaria la participación de expertos en los distintos dispositivos analizados que puedan identificar fallos en las mismas, formas más eficientes de implementar una determinada funcionalidad o mecanismos alternativos que mejoren la seguridad y eficiencia del dispositivo.

Típicamente deberán revisarse al menos dispositivos de electrónica de red (routers, switches, bridges, etc.), dispositivos de seguridad (cortafuegos/firewalls, IDS/IPS/dispositivos de prevención de intrusiones, servidores de autenticación, etc.), aplicaciones (servidores web, ftp, de correo, etc.) y en general cualquier dispositivo con una funcionalidad necesaria dentro de la organización que pueda suponer una posible fuente de vulnerabilidades y por tanto de elevación del nivel de riesgo asumido por la organización.

3.3.5 Visibilidad externa

Existe una gran cantidad de información relativa a las organizaciones accesible de forma pública desde Internet. Esta información puede ser una pieza clave para el diseño de un eventual plan de ataque contra la organización, ya que puede revelar interesantes detalles, tanto técnicos como organizativos, que utilizados de forma adecuada pueden facilitar la tarea de potenciales atacantes.

Es importante, por tanto, que la organización sea consciente de la existencia de esta información, por lo que deberá prestarse especial atención a los siguientes puntos.

3.3.5.1 Direccionamiento público

Mediante los servicios *whois* de los registradores regionales de Internet (e.g. RIPE en Europa, ARIN en Norteamérica) podemos conocer los rangos de direcciones públicas asignados a la organización, direcciones postales, de correo electrónico y números de teléfono, nombres de responsables y contactos dentro de la organización.

La organización deberá tener un conocimiento preciso de esta información con el fin de asegurarse que los datos son correctos y no proporciona más información de la debida.

3.3.5.2 Nombres de dominio y DNS

Deberán recopilarse todos los nombres de dominio pertenecientes a la organización, puesto que mediante las herramientas de consulta ofrecidas por los agentes registradores de dominio se pueden obtener datos de contactos técnicos, administrativos y de facturación.

Para cada dominio de la organización deberán realizarse búsquedas en el servicio DNS, prestando especial atención a:

- Servidores de Nombres (NS)
- Intercambiadores de correo (MX)
- Nombres conocidos (e.g. www, ftp)

Estos nombres, corresponderán a servidores susceptibles de ser atacados y por tanto deberán ser objeto de un cuidadoso proceso de asegurado.

3.3.5.3 Filtrado de documentación

Una mala configuración de los servidores web puede permitir la publicación en Internet de documentos que no deberían ser vistos fuera de la organización. Los actuales buscadores web (e.g. Google) permiten realizar sofisticadas búsquedas, por ejemplo restringidas por dominio y por tipo de fichero. Siempre resulta sorprendente la cantidad de información que puede ser hallada mediante estas búsquedas. Por tanto, dentro de la recolección técnica de información de la organización, deberán realizarse búsquedas de este tipo con el fin de conocer si la organización es vulnerable a este tipo de ataques e identificar cuál es la causa de esta publicación no autorizada.

3.3.6 Otros análisis técnicos

Adicionalmente, dependiendo de las características técnicas de la infraestructura de la organización, podrá ser necesaria la realización de otras pruebas para obtener información y datos adicionales. Estas pruebas deberán ser coordinadas e identificadas por el equipo de trabajo y los expertos en la tecnología, sistema o aplicativo objeto de las mismas.

3.4 *Análisis de Información*

Objetivo: Estudio y análisis de la información recolectada en las fases anteriores en base a códigos de mejores prácticas, estándares, normas, metodologías, conocimiento y experiencia del equipo de trabajo.

Tras haber realizado la recolección general y técnica de información según lo descrito en los anteriores apartados, se procederá al análisis de toda la información recogida y situaciones existentes, estudiando las posibles carencias en seguridad de la información de los productos, diseños de red, accesos a información o procesos organizativos implementados, entre otras cosas, tomando como base para ello distintas fuentes, entre las que se podrán destacar los códigos de buenas prácticas existentes aplicables a los distintos sistemas y procesos analizados, metodologías y estándares (como ISO 27001) de recomendable u obligado cumplimiento, legislación y normativas internas aplicables, además de bases de conocimiento existentes sobre los distintos sistemas o productos analizados y, por supuesto, la experiencia y conocimiento aportado por el equipo de trabajo encargado del proyecto.

En el desarrollo de este análisis será un activo crítico la experiencia y conocimiento del equipo de trabajo en las distintas áreas de la seguridad de la información aplicables, puesto que será objeto de su trabajo la identificación de posibles vulnerabilidades, fallos de concepto y debilidades en los diseños técnicos y de procesos de la organización, que requerirá un amplio conocimiento y experiencia en los campos analizados.

Este análisis supondrá el paso previo al desarrollo del Informe de Estado de la Seguridad de la Información en la Compañía (Informe SEIS) que, como se verá en el punto siguiente, desarrollará los distintos hallazgos y recomendaciones asociadas basándose para ello en dicho análisis.

3.5 Desarrollo de Informe SEIS (State of Enterprise Information Security, Estado de la Seguridad de la Información de la Compañía)

Objetivo: Elaboración del informe de estado de la seguridad de la información en la compañía que recogerá en un único documento una imagen de la situación actual de la organización en lo que a implantación de medidas técnicas y organizativa de la seguridad de la información se refiere.

A partir de los hallazgos obtenidos en la Recolección Técnica de Información, y tras haber procedido al análisis de toda la información recolectada, se desarrollará el informe SEIS (*State of Enterprise Information Security*). Este informe persigue dos objetivos. El primero, proporcionar una visión global y detallada del estado de la organización en cuanto a la seguridad de la información. El segundo objetivo, no menos importante, es señalar cuales son los aspectos mejorables que atañen a la seguridad de la información así como proponer acciones correctivas priorizándolas de acuerdo con la relevancia que tengan para la organización.

A continuación se detallarán los distintos apartados que componen el informe SEIS.

3.5.1 Descripción del estado actual

En este apartado se describirán los hallazgos obtenidos durante la Recolección Técnica de Información y el estado actual de las redes y sistemas de información de la organización. Un ejemplo de la estructura de este apartado sería el siguiente:

- Topología: Descripción de la topología de las redes de la organización. Recopilación de esquemas físicos y lógicos
- Sistemas: Inventario y caracterización de los sistemas más importantes de la organización.
- Servicios: Inventario y caracterización de los servicios públicos y privados de la organización.
- Seguridad Física: Descripción de las medidas de seguridad física implantadas en las dependencias de la organización.
- Seguridad Lógica: Descripción de las medidas de seguridad lógica implantadas en la organización para proteger sus sistemas de información.
- Gestión y Operaciones: Listado de las políticas y procedimientos existentes en la organización referentes a manejo de sistemas de información.

3.5.2 Análisis y Recomendaciones Técnicas

Para cada uno de los apartados indicados en el apartado anterior y siguiendo la misma estructura en su documentación, se revisarán las implicaciones existentes respecto a la seguridad de la información y se recomendarán las acciones necesarias para paliar los problemas encontrados.

3.5.3 Conclusiones y Propuestas de acción

En este apartado, se ordenarán las acciones recomendadas en el apartado anterior según una gradación basada en la criticidad de su aplicación. Dicha criticidad, se asignará teniendo en cuenta la cantidad de riesgo que la ausencia de aplicación de la acción tendría sobre la organización. Este riesgo, no siempre debe ser calculado de manera objetiva (i.e. pérdida monetaria), sino que en muchos casos dependerá de otras consideraciones propias de la organización.

Deberá prestarse especial atención a las acciones consideradas como extremadamente prioritarias debido a que suponen un riesgo inmediato que no puede ser asumido por la organización. Para todas las acciones recomendadas se especificará un tiempo recomendado para abordar su aplicación según su grado de riesgo. Como referencia, un ejemplo de gradación podría ser el siguiente:

- Crítico: Aplicación inmediata
- Alto: Aplicación en tres meses
- Medio: Aplicación de tres a seis meses
- Bajo: Aplicación de seis a doce meses

3.5.4 Medidas de Seguridad y Controles Recomendados

Adicionalmente, se propondrán una serie de medidas y controles de seguridad aplicables tal como se recomiendan en las guías de buenas prácticas existentes en este campo. IS2ME no requiere la utilización de ninguna norma específica, si bien, su filosofía y objetivo se ajusta a lo propuesto por la norma ISO/IEC 17799/27001.

En este punto se recomienda la identificación y descripción de las distintas medidas de seguridad y controles aplicables de la norma seguida, de forma que esta parte del informe pueda servir como referencia para su posterior implantación que, evidentemente, requerirá de un desarrollo posterior en profundidad de cada uno de esos controles en la fase de Implantación de IASAP.

3.5.5 Resumen Ejecutivo

Deberá desarrollarse como un apartado más del informe, un resumen ejecutivo que recogerá de forma clara, concisa y en un lenguaje fácilmente comprensible, evitando términos excesivamente técnicos en la medida de lo posible, un resumen de los principales resultados y riesgos que la organización está asumiendo debido al estado actual de implementación de medidas, en lo que a seguridad de la información se refiere.

Deberá prestarse especial atención al desarrollo de este apartado, puesto que probablemente sea el que mayor visibilidad vaya a tener en la organización y, por tanto, el que pueda influir de forma decisiva en la continuidad del apoyo gerencial hacia el cumplimiento de las medidas necesarias y en la incorporación de la seguridad de la información a la cultura organizacional de la compañía.

3.6 Presentación de Informe SEIS a Alta Dirección

Objetivo: Presentación del Informe de Estado de Seguridad de la Información de la compañía a la alta dirección, suponiendo ello un hito para la asunción de la seguridad como un requisito de negocio más en la cultura organizacional de la compañía.

El desarrollo del Informe SEIS como materialización documentada de la recolección técnica y general de información ya indicada anteriormente, persigue un doble objetivo. Por un parte conformar una documentación que recoja de forma concisa y clara el estado, tanto técnico como organizativo, de la organización en el campo de la seguridad de la información, lo que en sí mismo, suponga un activo importante para la organización que pueda ser utilizado, en adelante, como documentación de referencia (probablemente tras sesgar cierta información clasificada como confidencial) para la petición de ofertas a proveedores, documentación de soluciones, etc.

Sin embargo, el segundo objetivo (probablemente el más importante), sea el de servir como referencia (especialmente el resumen ejecutivo) a la alta dirección para el apoyo en la toma de decisiones relativas a la disminución del riesgo asumido por la compañía y, por tanto, al aumento del valor de la misma.

En este sentido deberá realizarse una presentación del mismo a la alta dirección de la compañía para lo que deberá identificarse claramente cuáles son los mensajes claves que desean transmitirse a la misma, siempre desarrollando esos mensajes en un lenguaje familiar que se corresponda con la terminología, no tanto técnica, sino de negocio y de riesgos financieros y que permita a los asistentes a la presentación una fácil comprensión de los mensajes transmitidos.

La presentación deberá estructurarse adecuadamente, para lo cuál se recomienda un esquema similar al siguiente:

- Muy breve introducción sobre seguridad de la información
- Descripción del estudio realizado y motivación del mismo
- Estado actual de la organización
- Ejemplos reales de hallazgos, problemas y/o vulnerabilidades existentes
- Recomendaciones
- Acciones inmediatas requeridas
- Conclusiones

Se recomienda que tanto en la parte inicial de la presentación (estado actual) como en la final (conclusiones) se indique clara y explícitamente el nivel de riesgo asumido por la organización mediante unas afirmaciones breves y concisas como “El nivel de riesgo es Alto e Inaceptable en una organización de esta dimensión y visibilidad” o “la estructura organizativa es mejorable y existe un Nivel Insuficiente de medidas de seguridad técnicas y organizativas”, por ejemplo.

La duración de la presentación dependerá de la dimensión de la organización, la naturaleza de la información a presentar y otras consideraciones (como disponibilidad del equipo directivo, etc.), sin embargo se recomienda que se reserve para la misma un espacio de tiempo entre 1 y 2 horas. Al final de la presentación deberán reservarse unos minutos para la realización de “comentarios libres”, preguntas y dudas de los asistentes, justificaciones o desarrollo en detalle de alguna cuestión que los asistentes puedan requerir.

El resultado de esta presentación debería materializarse en el apoyo y compromiso explícito de la alta dirección en el desarrollo de la continuación del proyecto y en la aprobación del informe SEIS que suponga la aprobación para comenzar el desarrollo del Documento IASAP (Plan de Acción de Seguridad de la Información, Information Assurance and Security Action Plan).

3.7 Desarrollo del Documento IASAP (Information Assurance and Security Action Plan, Plan de Acción de Seguridad y Protección de la Información)

Objetivo: Elaboración del documento Plan de Acción de Seguridad y Protección de la Información como base para la posterior implantación de acciones correspondientes en la organización y elaboración de los Planes de Seguridad de la Organización.

Una vez recibida la aprobación por parte de la alta dirección del Informe SEIS, lo que deberá incluir de forma explícita la aceptación de desarrollo del documento IASAP (Information Assurance and Security Action Plan, Plan de Acción de Seguridad y Protección de la Información), se comenzará la tarea de elaboración del documento abordando en detalle cada una de las acciones propuestas en el Informe SEIS.

La información es uno de los activos más importantes para la organización que, como otros recursos de la misma, tiene un gran valor y por consiguiente debe ser debidamente protegida. El objetivo de la seguridad de la información es proteger a ésta de una amplia gama de amenazas, a fin de garantizar la continuidad de la actividad de la organización, minimizar el daño a la misma y maximizar el retorno sobre las inversiones y las oportunidades, teniendo como objetivo la preservación de la confidencialidad (garantizando que la información sea accesible sólo por aquellas personas autorizadas a tener acceso a ella), integridad (salvaguardando la exactitud y totalidad de la información y, en su caso, los métodos de procesamiento de la misma) y la disponibilidad (garantizando que los usuarios autorizados tengan acceso a la información y los recursos correspondientes siempre que se requiera).

La seguridad de la información se consigue implementando un conjunto adecuado de controles y medidas de seguridad que abarcan políticas, procedimientos, prácticas, estructuras organizacionales o funciones del software, entre otras, que garanticen los objetivos específicos mencionados anteriormente. En el diseño o desarrollo de muchos sistemas de información, en algunos casos, no se tienen en cuenta requisitos o características de seguridad adecuadas. Por ello, la seguridad que puede lograrse por medios técnicos es limitada y debe ser apoyada por una gestión y procedimientos adecuados, participando todos los empleados de la organización, e incluso en algunos casos, proveedores y usuarios o clientes.

Es esencial, por tanto, que la organización identifique sus requisitos de seguridad mediante la evaluación de los riesgos a los que se enfrenta, además de identificar los requisitos legales, normativos, reglamentarios y contractuales que debe cumplir, y los principios, objetivos y requisitos para el procesamiento de la información que ha desarrollado para respaldar sus operaciones.

Una vez identificados los requisitos de seguridad, deben seleccionarse e implementarse las acciones y medidas de seguridad adecuadas para reducir los riesgos a un nivel aceptable. Estas acciones y medidas de seguridad serán las identificadas inicialmente en el informe SEIS y serán desarrolladas en detalle, incluyendo recursos necesarios para su implementación, planificación o valoración económica cuando corresponda, en el documento IASAP.

Este documento conformará el Plan de Acción de Seguridad de la Información de la compañía que incluirá de forma general la planificación completa para la implementación de las acciones identificadas de forma que puedan establecerse unos hitos y fechas asociadas para el cumplimiento y consecución de determinados objetivos a nivel de organización, departamento o incluso personal en la compañía, y particularmente para cada una de las acciones, al menos la siguiente información:

- Desarrollo técnico (y organizativo cuando corresponda) completo y en detalle de la acción.
- Planificación completa y detallada de cada acción, incluyendo tiempos y plan de implantación (corto, medio y largo plazo).
- Identificación de recursos humanos necesarios, incluyendo explícitamente si deben o pueden ser internos o externos.
- Valoración económica en aquellos casos que pueda realizarse (tanto si se trata de acciones realizadas por proveedores externos como si deben realizarse internamente).
- Ofertas de proveedores en aquellas acciones que requieran de un tercero para su implementación.

Las acciones a incluir dentro del documento IASAP dependerán de las medidas de seguridad que la compañía ya tuviese implementadas y del grado de "impregnación" de la seguridad de la información en la cultura organizacional de la compañía si bien, como orientación, algunas de las acciones que habitualmente serán incluidas podrán ser:

- Mejora de la estructura organizativa de la compañía (establecimiento de comité de seguridad, asignación de responsabilidades, etc.)
- Posible externalización de algunas funciones IT
- Desarrollo y difusión de políticas de seguridad y procedimientos asociados
- Mejoras en las plataformas de sistemas o en el centro de proceso de datos
- Mejoras en la seguridad de los dispositivos de comunicaciones (redes inalámbricas, WAN, LAN, segmentación de redes, etc.)
- Análisis de vulnerabilidades
- Desarrollo del proceso de gestión de la continuidad del negocio
- Análisis de riesgos
- Desarrollo del plan de contingencia IT
- Plan de formación
- Otros

En algunos casos será necesario, e incluso aconsejable, el contacto con terceras partes expertas en determinada área, o la petición de oferta a proveedores para el correcto dimensionamiento tanto en recursos humanos como económicos de algunas de las acciones necesarias.

3.8 Presentación del Documento IASAP a Alta Dirección

Objetivo: Presentación del Plan de Seguridad y Protección de la Información a la Alta Dirección para su aprobación, sentando así la base para su posterior implantación.

Finalizado el documento IASAP deberá realizarse la presentación y defensa del mismo a la alta dirección. Esta presentación deberá haber sido planificada con anterioridad en la misma presentación del informe SEIS y establecerá una continuidad en el proyecto de implantación de la seguridad objeto de este método.

La aprobación del documento IASAP por la alta dirección supondrá un hito crucial en el compromiso de la organización en la inclusión de la seguridad de la información en todos sus procesos, puesto que en caso afirmativo, esta aprobación supondrá el comienzo del Plan de Acción de Seguridad de la Información según las características, planificación y estimación de recursos humanos y económicos correspondientes.

Será en este punto cuando la alta dirección cuente con toda la información para valorar en su justa medida los esfuerzos necesarios que la organización deberá tomar para cumplir sus objetivos de disminución del riesgo y mejora de sus niveles de seguridad, juzgando la conveniencia de los plazos y acciones propuestas en el documento IASAP y ajustando o modificando los mismos teniendo en cuenta otras consideraciones adicionales que en algunos casos puede aportar únicamente este nivel de dirección como estrategias globales de negocio, sinergias existentes con otras organizaciones, etc.

Para la realización de la presentación, al igual que en el caso de la presentación del Informe SEIS, deberá tenerse en cuenta que es muy probable que la audiencia no tenga una formación técnica en el campo de la seguridad y por tanto deberá enfocarse el mensaje adecuadamente. Para ello serán de aplicación todas las recomendaciones ya efectuadas en el punto "Presentación del Informe SEIS a Alta Dirección".

Se incluye a continuación a modo de ejemplo, y como referencia, una posible estructura de la presentación del documento IASAP:

- Introducción sobre el origen del documento IASAP y el proceso de desarrollo asociado.
- Descripción temporal y justificada del corto, medio y largo plazo describen el tipo de acciones y su razón para ser incluidas en dichos plazos

- Planificación general: identificación de todas y cada una de las acciones a realizar a corto, medio y largo plazo.
- Corto Plazo: descripción detallada de cada acción a realizar en este plazo incluyendo plazo temporal de implantación, recursos necesarios (indicando explícitamente si son internos y/o externos), propuestas de proveedores cuando aplique, tareas incluidas y valoración económica (por ejemplo, aquellas tareas con un plazo de cumplimiento inferior a 6 meses).
- Medio Plazo: descripción detallada de cada acción a realizar como se ha indicado anteriormente (de 6 a 12 meses).
- Largo Plazo: descripción detallada de cada acción a realizar como se ha indicado anteriormente (más de 12 meses).²
- Propuesta de Planificación Temporal: propuesta con fechas reales objetivo de cumplimiento del documento IASAP (traslado de la planificación propuesta al calendario real con propuesta de fechas para hitos, finalización de acciones, etc.).

Además de todas las mejoras aportadas en el campo de la seguridad, el establecimiento del documento IASAP como marco de implementación de las acciones indicadas podrá suponer una base sobre la que establecer una política de cumplimiento de objetivos a distintos niveles de la organización desde las distintas direcciones, áreas o departamentos, hasta el establecimiento de objetivos individuales asociados a distintas personas o roles existentes.

3.9 Implantación de IASAP

Objetivo: Desarrollo e Implantación del Plan de Acción de Seguridad y Protección de la Información según la planificación propuesta en el mismo.

Una vez presentado el documento IASAP, y aceptado éste por la dirección, llega el momento de realizar la implantación de las diferentes tareas identificadas en el Plan de Acción de Seguridad de la Información. Si bien, el personal involucrado en el desarrollo de las diferentes fases del método IS2ME no tiene por qué estar dedicado a la implantación de estas tareas, sí es importante, que realice labores de seguimiento y coordinación de las mismas, con el fin de asegurar que los objetivos son cumplidos y los controles implantados correctamente. Este es un paso trascendental, ya que la correcta realización de las tareas propuestas permitirá iniciar el largo camino del cumplimiento e implantación de un sistema de gestión de la seguridad de la información ISO 27001. Momento en el que se podrá abordar una aproximación tradicional para el mantenimiento de la seguridad de la información dentro de la organización.

Para realizar la implantación de IASAP, se desarrollará un plan de proyecto de coordinación de la implantación que incluirá:

- **Adquisición/Asignación de recursos necesarios:** Estos recursos han sido claramente identificados en el plan IASAP, ahora es el momento de realizar la asignación de dichos recursos a las tareas que se van a llevar a cabo. Deberá asegurarse la disponibilidad de los mismos en los plazos estimados, y la posibilidad de que algunos de ellos puedan ser asignados a tareas que se realicen de forma simultánea.
- **Seguimiento:** Las labores de seguimiento servirán para asegurar que las tareas especificadas en el plan de acción se realizan diligentemente y dentro de los plazos estipulados. El personal encargado del seguimiento deberá coordinar el trabajo entre los equipos que realicen tareas en sistemas con interfaces comunes para verificar que las mejoras implantadas no interfieran unas con otras.

² Estos plazos son orientativos. Los plazos a definir son aquellos que cumplan los objetivos marcados y se alineen con la estrategia de negocio existente en la organización.

- **Reuniones de Revisión:** Se programarán reuniones de revisión periódicas así como reuniones con la dirección para informar del estado del desarrollo de la implantación de las diferentes tareas.

4 Conclusiones

En los últimos tiempos, el mundo empresarial ha comenzado a ser consciente de la necesidad de incorporar seguridad a las organizaciones. Esta tarea es ardua y no trivial, afortunadamente existen metodologías que facilitan el desarrollo de los procesos orientados a la incorporación de la seguridad. No obstante, la mayor parte de las veces, estas metodologías suponen que las organizaciones tienen una entidad, recursos y trabajo previo realizado, lo cual no es aplicable a la mayoría de las empresas existentes.

Los autores consideramos que IS2ME viene a llenar un vacío existente en la implantación de la seguridad en pequeñas y medianas empresas, permitiendo, al contrario que las metodologías tradicionales, la obtención de resultados de forma rápida y con una razonable utilización de recursos. Estos resultados significarán una disminución del riesgo que afronta la organización, la desaparición de gran cantidad de problemas técnicos y organizativos, y una base firme para desarrollar la implantación de los mecanismos de seguridad necesarios que permitan afrontar la completa implantación de un sistema de gestión de la seguridad de la información.