Gestión estratégica de seguridad en la empresa

anetcom

Gestión Estratégica de Seguridad en la Empresa

anetcom

Edita:
Anetcom

Creación de contenidos:
GMV
Javier Megias Terol
Javier Osuna García Malo de Molina
Roberto López Navarro
Antonio Cabañas Adame
Nathalie Dahan García
Mariano J. Benito Gómez
Luis Miguel Simoni Granada

Coordinación:
Javier Megias Terol
Olga Ramírez Sánchez

Colaboración:
José Luis Colvée

Revisión:
Inmaculada Elum
Carolina Izquierdo

Diseño editorial:
Filmac Centre S.L.

Imagen de portada, maquetación y composición:
Integral Comunicación

Impresión:
Gráficas Marí Montañana

Depósito legal:
V-973-2008

Índice

Prólogo 7

1. Introducción 11
1.1. Panorama actual y desafíos para la empresa en seguridad 15
1.2. Seguridad y estrategia: una introducción práctica al buen Gobierno Corporativo TI 18

2. Planificación de la seguridad 25
2.1. Estableciendo los cimientos de la estrategia: la política de seguridad y la organización 25
2.2. Gestión del riesgo: ¿cuánto cuesta la seguridad? 29
2.2.1. Identificación de activos: el corazón del negocio 32
2.2.2. Amenazas de seguridad y vulnerabilidades 34
2.2.3. El riesgo como factor de la seguridad 36
2.2.4. Algunas realidades en la Gestión del Riesgo 38
2.3. Abordando de forma práctica la planificación de la seguridad en la empresa: el plan director de seguridad 42
2.4. La seguridad en las TIC: requisitos básicos 49
2.4.1. La seguridad lógica 50
2.4.2. Componentes de la defensa en profundidad 54
2.4.3. Seguridad en el perímetro 55
2.5. Gestión de la continuidad y recuperación de desastres 65
2.5.1. Entendimiento del negocio 69
2.5.2. Definición de la estrategia de respaldo y continuidad 71
2.5.3. Desarrollo del plan de continuidad 72
2.5.4. Mantenimiento del plan 73
2.6. Cumplimiento legal: LOPD, LSSI y otras regulaciones 73
2.7. Gestión de las auditorías, o cómo evaluar la realidad 79
2.8. Cuadros de mando, métricas e indicadores: midiendo la seguridad 83
2.9. Buenas prácticas de externalización de seguridad 88

3. Marcos de referencia para la Gestión Estratégica de la Seguridad **93**
3.1. Sistemas de Gestión de Seguridad (SGSI): ISO 27001 e ISO 17799 **94**
3.2. Gobierno Corporativo y Seguridad: COBIT **101**
3.3. Gestión de Servicios TI: ITIL/ISO 20000 **104**

4. Referencias **109**

5. Bibliografía **111**

Prólogo

La Seguridad de los Sistemas de Información es actualmente una de las principales preocupaciones de los ciudadanos, empresas y profesionales de todo el mundo. La confianza en los servicios telemáticos, elemento clave para el desarrollo de una Sociedad de la Información sana está en entredicho.

En los últimos tiempos proliferan las amenazas, que van desde los virus informáticos hasta el "ciberterrorismo", pasando por la usurpación de identidades bancarias o el robo de información confidencial. Resulta demoledor el efecto producido por estos peligros, en usuarios y ciudadanos en general, por lo que respecta a la percepción de la seguridad en medios telemáticos.

Conscientes de esta preocupación, desde instituciones como la Generalitat Valenciana hemos promovido iniciativas que garanticen la Seguridad de la Información. De este modo, desde el Gobierno Valenciano y en concreto desde la Conselleria de Justicia y Administraciones Públicas hemos impulsado el Centro de Seguridad TIC de la Comunidad Valenciana (CSIRT-CV), un proyecto que se enmarca en el Plan Estratégico de Telecomunicaciones Avanzadas (AVANTIC) y que ha sido recientemente inaugurado. El CSIRT-CV se creó para prevenir incidentes, en materia de seguridad informática, así como para establecer las medidas más adecuadas para detectar, estudiar y evitar las amenazas.

No obstante, existen todavía empresas que carecen de orientación sobre los ajustes que deben realizar en su negocio para proteger adecuadamente sus sistemas de información o que desconocen la existencia de los mismos. En este sentido, debemos insistir en el conocimiento, difusión e implantación de cuantos medios sean necesarios para garantizar la seguridad informática del tejido empresarial.

Sobre los contenidos de esta interesante y necesaria publicación, de la editorial de Anetcom, que han sido redactados por expertos en seguridad de los sistemas de

información de GMV, a los que desde aquí felicito por el resultado de este manual, tengo que señalar que el libro recoge una serie de buenas prácticas, planteamientos y herramientas útiles sobre esta materia para empresarios y directores de informática.

El objetivo de estas propuestas no es otro que el de ayudar a los directivos de las empresas a orientar, desde un punto de vista estratégico, la gestión en materia de Seguridad de la Información. Este nuevo enfoque permite, tal y como señalan los técnicos, planificar con antelación la protección de la empresa, entender las consecuencias y el coste económico de cada decisión y, sobre todo, poder afrontar las inversiones de forma comprensible y justificada.

En este sentido, la publicación abarca un planteamiento que va más allá de la tecnología y que no se centra, únicamente, en el plano técnico –como se había considerado hasta ahora– sino también desde la gestión, analizando el conjunto de la empresa.

De este modo, el planteamiento buscado por Anetcom y los autores del libro abarca la temática aquí analizada desde una perspectiva más allá de la tecnología y del proceso, ampliando el análisis a otros aspectos como la cultura empresarial y profesional. De nuevo Anetcom acerca estos conceptos a la realidad empresarial y éste es el mensaje de cercanía que queremos transmitir desde el Gobierno Valenciano.

Fernando de Rosa

Conseller de Justicia y Administraciones Públicas

Introducción

Definitivamente era muy extraño. Eran las nueve de la noche del jueves, y reflexionando acerca de lo sucedido esa tarde, Juan se sentía cada vez más intranquilo. El presidente de su empresa, el señor Llopis, lo había convocado a una reunión sorpresa para las diez de la mañana del día siguiente. Aún recordaba mentalmente la escueta nota dejada sobre una esquina de su abarrotada mesa: "Juan, necesito una explicación de por qué hemos gastado miles de euros durante este año en seguridad informática, y aún así solicitas un incremento del presupuesto para el próximo año".

Desde que asumió hace algunos años la dirección de informática de la empresa, Juan creía haber hecho un buen trabajo modernizando los sistemas de la compañía y, aunque había gastado grandes sumas, nunca se había visto en esta situación. ¿A qué se debía que el señor Llopis quisiera hablar justo entonces de esa partida presupuestaria? No era en absoluto de las más grandes que había solicitado, y tampoco recordaba haber tenido ninguna infección de virus ese año… Eso sí, por si acaso y en previsión de posibles nuevos problemas, había pedido un aumento del 15%, completamente razonable.

Resignado, abrió un documento y comenzó a desglosar metódicamente el presupuesto que había gastado durante el año. Tras media hora, una creciente sensación de pánico se fue apoderando de Juan: la conciencia de que todo lo que había invertido ese año había sido consecuencia de una respuesta urgente a un problema (el *antispam* en enero, la actualización del antivirus en marzo...), o de actuaciones a las que les había obligado la dichosa Ley de Protección de Datos se fue abriendo camino... y se dio cuenta que apenas había podido planificar nada. ¿Qué le dirá Juan al señor Llopis cuando le pregunte por la estrategia adoptada para la inversión en seguridad?

A las organizaciones que operan en esta época sin duda les ha sido dado vivir tiempos interesantes. Cada vez más, los procesos de negocio crecen en complejidad, y a la vez aumenta la dependencia de los mismos hacia la tecnología (más marcada si cabe en ciertos sectores). Por contraposición, las mismas organizaciones se enfrentan a un crecimiento paulatino de exigencias, tanto en el plano regulatorio como en de la eficiencia (costes y tiempo). Esta situación nada halagüeña se ve empeorada por multitud de amenazas hacia los activos que soportan dichos procesos. Pero, a pesar de que históricamente diversos actores asociados al mercado de la Seguridad de la Información han basado sus preceptos comerciales en el miedo, cada vez resulta más patente lo caduco de este planteamiento.

En esta situación, hoy en día no son pocas las organizaciones que adolecen de una visión y conciencia clara de la importancia de que sus servicios y procesos, cimentados en la tecnología o no, se relacionen y operen de forma segura. Aun así, existen dificultades para engarzar esta visión con unas dotaciones presupuestarias apropiadas, o dicho de otra forma, para interpretar y poder razonar apropiadamente los gastos (o, mejor inversiones) que inevitablemente se producirán.

En primer lugar, es primordial abandonar la visión reduccionista y entender que la Seguridad de la Información abarca varias áreas convergentes pero con foco común. En numerosas ocasiones su ámbito excede a la tecnología, e incluye otros enfoques asociados a la estructura organizativa de la empresa, al cumplimiento de las regulaciones (sectoriales o globales) o incluso a la forma en que los procesos de negocio operan. Es fundamental pues adoptar una visión holística e integrada de la Seguridad de la Información para poder ofrecer una respuesta completa, eficiente y conmensurada a las necesidades de protección y seguridad de la organización.

El corazón de este enfoque no debe ser sólo la tecnología, tal como se ha venido planteando hasta ahora (servidores, *software* u otros activos). El elemento esencial que permite que la empresa prospere y que representa su principal capital es la **información**, y alrededor de ella es donde se debe construir la seguridad.

Ilustración 1.- Seguridad de la Información: un enfoque global.

En este punto nace la intuición de que el enfoque correcto no puede situarse en un plano puramente operativo o táctico: tiene implicaciones demasiado relevantes en el rumbo que sigue la empresa y afecta de forma profunda y horizontal a la operativa de la organización. El planteamiento apropiado debería alinearse con el negocio y tratarse desde una dimensión estratégica, superando las barreras del presente para entender cuáles serán los requisitos de la organización para el futuro, pudiendo así cumplir su objetivo: **entregar valor** de forma clara y, sobre todo, mesurable.

¿Pero están las organizaciones de hoy en día preparadas para este cambio de mentalidad? La respuesta variará de forma ostensible atendiendo a varios factores: el negocio de la empresa, su cultura interna, la orientación a la mejora o incluso la flexibilidad de sus procesos. En cualquier caso, en este punto se hace patente que la seguridad debe ser **planificada alineándola con la estrategia de la empresa**, y fundamentada en metodologías claras y medibles. Este

cambio de paradigma supone dejar atrás la seguridad basada en intuiciones o reacciones, y construirla desde un nuevo enfoque: el de la estrategia. Esta construcción, clave para un buen comienzo, se debe basar en tres puntos principales:

- El **autoconocimiento** de las necesidades de protección de los procesos de negocio, para lo cual es importante interiorizar y entender la distinción entre lo que aporta valor y lo que no lo aporta.

- El **origen** o punto del que se parte, y el nivel de **compromiso** de la organización (factor clave, y al que este libro dedica un capítulo).

- El **destino** o dónde se quiere llegar, ya sea en términos cualitativos o cuantitativos, pero en todos los casos con la mejora continua como camino.

Con estos datos se puede definir un camino basado en una planificación clara, tangible y, sobre todo, medible. Para ayudar a las organizaciones a construir este camino hoy en día existen numerosas normas y guías de buenas prácticas, que resultan de gran ayuda. Aun así, es importante advertir que dichas normas, vistas en conjunto y si no se posee un conocimiento profundo sobre ellas, pueden representar una tupida malla que podría hacer perder el foco a la empresa. En consecuencia, será imprescindible no dejarse llevar por modas y aplicar el sentido común en su implantación, usando únicamente las partes más apropiadas para la organización.

Asimismo, es importante no olvidar que el objetivo último de cualquier área de Sistemas de Información (excepto en empresas cuyo negocio son los propios procesos TIC), es **apoyar** al resto de procesos productivos de la empresa, aportando valor y cuando sea posible, reduciendo el coste de los servicios que soportan (ya sea monetario o temporal).

Tras todo lo expuesto, empieza a resultar claro que para conseguir los pingües beneficios que ofrece este cambio, es imprescindible además hacer una profunda reflexión sobre la propia organización: ¿Cuál es el ritmo al que puede cambiar la empresa? ¿Se dispone internamente de todos los conocimientos necesarios para acometer este cambio o se deberá buscar ayuda fuera? ¿El personal que debe cambiar de paradigma y comenzar a gestionar la seguridad puede (y quiere) hacerlo?

Dado el escenario planteado, en el que se han hablado de dotaciones presupuestarias adicionales, cambios organizacionales, nuevos enfoques de gestión y diversas normas y procesos de referencia, es fácil caer en el desánimo y continuar en el camino de menor resistencia, la reactividad. Pero, para aquellas organizaciones que tengan la paciencia y valentía de seguir profundizando en la gestión estratégica de seguridad, se abrirán nuevas oportunidades, un idioma común de negocio y un entendimiento claro de **en qué** y **por qué** se gasta cada euro dedicado a la seguridad.

En resumen, el objeto de este libro es acompañar tanto al Director de Sistemas de Información (CIO según los parámetros anglosajones), que se plantea dar el paso hacia la Gestión Estratégica de la Seguridad, como al profesional de la seguridad, consciente de que puede aportar más valor a su organización. También servirá, sin duda, como orientación para el Director Gerente (CEO), que busca un modelo que le permita reducir la complejidad de su gestión de TI y seguridad, a la vez que consigue que ésta se convierta en un proceso comprensible y alineado con el negocio de su empresa.

◆ 1.1. Panorama actual y desafíos para la empresa en seguridad

Existen diversos desafíos o retos de carácter estructural a los que se enfrentan actualmente las organizaciones y que es importante conocer. Conocimiento es anticipación en este nuevo paradigma. Uno de los principales desafíos es la imperiosa necesidad de adoptar una visión global de la seguridad en sus servicios y procesos. Para ello no es suficiente la mera supervisión de los requisitos puntuales de seguridad en determinados sistemas o aplicaciones, sino que se debe disponer de controles engarzados en los procesos de negocio que soportan la organización. Este punto lleva al primer cambio esencial que debe afrontar la percepción de la organización: la seguridad debe pasar de la clásica concepción de "mal necesario" hacia su visión como un **factor habilitador de negocio** más que facilita la confianza en la organización.

Quizás este último aspecto merece una mayor reflexión: los clientes (o usuarios) de la organización también han evolucionado, y cada vez más valoran la confianza y otros aspectos, percibidos como diferenciadores y necesarios:

- Confidencialidad de las relaciones y operaciones con la organización que le presta servicios o de quien adquieren productos.

- Habilidad de poder seguir prestando servicios o produciendo ante una amenaza a la continuidad del negocio.

- Posibilidad de relacionarse mediante canales alternativos (movilidad, firma electrónica, telefonía…) con las mismas garantías que ofrecen los entornos tradicionales.

También es necesario recordar y destacar el aumento de complejidad en los negocios y los entornos TIC que los soportan, así como las nuevas formas de trabajo, significativamente más cómodas pero con requisitos de seguridad notablemente complejos (desde teletrabajo hasta la movilidad). Las palabras clave que deben definir el papel de la seguridad en esta situación son **flexibilidad y adaptación**.

Ciertos controles de protección están parcialmente recogidos por diversas regulaciones y normativas, como las relativas a la protección de datos de carácter personal. Pero la realidad es que el alcance del cambio de paradigma debe ir mucho más allá, ya que tiene que ver con el activo principal que diferenciará a la organización: la **confianza**. La percepción de la importancia e impacto de la confianza en las relaciones con los clientes/usuarios varía aunque su necesidad es considerada un hecho en sectores como el financiero o el sanitario, y sólo se intuye su relevancia en otros muchos. En todos los casos, la relación entre la Gestión de la Seguridad y la confianza es de carácter intrínseco y no debería ser subestimada.

Dicho esto, y tras esta exhortación para apreciar justamente el valor de la Gestión de Seguridad en la organización, subyace otra consideración no menos importante: la seguridad debe quedar subordinada a la operativa de la empresa. Aunque quizás evidente, no deben existir controles que impidan o dificulten el buen rendimiento de los procesos y servicios de la organización, a menos que su justificación sea clara (ya sea por imperativo legal, norma de la industria o necesidad justificada).

Es precisamente en los aspectos normativos donde se adivinan los principales mimbres sobre los que se deberá construir la estrategia de cumplimiento y gestión de la organización en los próximos tiempos. En cierto número de sectores, como el financiero, ya existen regulaciones que no sólo incentivan o incluso obligan a que la alta dirección conozca y sea consciente del riesgo al

que se enfrenta su organización, sino que además ésta debe aceptar por escrito dicho nivel de riesgo. Las ramificaciones de este hecho son abrumadoras, dado que para cumplirlas es imprescindible un alto nivel de apoyo y compromiso de las áreas de dirección, lo que a su vez condicionará el planteamiento de la Gestión de Seguridad. En este nuevo enfoque no es aceptable que responsables de un área técnica únicamente hablen de elementos de carácter puramente operativo (como por ejemplo los virus), sino que deberán transformarse en estrategas que planteen sus movimientos en base a los factores de riesgo que afectan a los procesos de negocio, justificando y planificando las acciones necesarias para mitigar dichos riesgos.

Este cambio supondrá que un cierto número de profesionales no serán capaces de completar la transición que los llevará de un área puramente operativa y reactiva a una de carácter marcadamente estratégico, lo que a su vez exigirá un conjunto de conocimientos y habilidades diferentes y adicionales a los previamente existentes.

En esta nueva era de seguridad, que en determinadas organizaciones ya es presente, las áreas de seguridad deben, al igual que el resto de áreas que aportan valor a la empresa, poder justificar, tanto a nivel económico como operativo cada decisión, y poder controlar su rendimiento. Para ello, instrumentos históricamente asociados a áreas diferentes, como las financieras, pasarán a convertirse en herramientas para la gestión estratégica de seguridad.

Entre ellas, pueden citarse como las más relevantes los Cuadros de mando, los Planes Directores y Sistemas de Gestión Integrada. Asimismo, estas mismas herramientas, que ayudarán a controlar la Gestión de la Seguridad en la organización, deberán ser capaces de ofrecer información a varios niveles. Otra de las claves que marca la Gestión Estratégica de la Seguridad es la disponibilidad de información estratificada y segregada según su destinatario y ámbito, con el fin de ofrecer información de carácter operativo a las áreas técnicas, datos de rendimiento de los procesos a los responsables de servicios e información de gestión a los miembros de las áreas ejecutivas.

Finalmente, y como consecuencia de esta orientación a la mejora continua en la seguridad, la medición del nivel de madurez en el que opera la organización se convierte en un punto de alta relevancia. Cobra esta importancia no sólo por su carácter de meta sino porque su estandarización permitirá a

diferentes compañías de sectores similares comparar su gestión (lo que en muchos casos se considera útil pero no deseable).

1.2. Seguridad y Estrategia: una introducción práctica al buen Gobierno Corporativo TI

El Gobierno Corporativo TI, término que nace del anglosajón IT Governance, es una disciplina de gestión que se integra en las prácticas de Gobierno Corporativo de la organización. Su fin es ofrecer un marco para ayudar a que las áreas de TI se alineen y cumplan con los objetivos del negocio, demostrando con información contrastada el impacto positivo de las inversiones realizadas, o dicho de otra forma, es la "profesionalización" de la gestión de TI para asegurar la creación de valor.

Esta disciplina comienza a tener una mayor difusión como consecuencia de los escándalos financieros acaecidos a lo largo de 2002, y nace con el objetivo de ofrecer confianza a accionistas e interesados en la gestión de la empresa y, en el caso específico de la tecnología, reducir el abismo que existe habitualmente entre las expectativas de la organización para las áreas de TI y los resultados ofrecidos. En EE.UU. tuvo una derivada adicional: la creación de la ley federal Sarbanes-Oaxley Act (también conocido como SOX), cuyo fin es definir requisitos de gestión, y supervisar las compañías que cotizan en bolsa en EEUU, haciendo especial hincapié en la aplicación de controles.

Uno de los principales puntos a los que hace referencia el Gobierno Corporativo de TI es la obligatoriedad de conocer y controlar el **riesgo operativo**, término heredado de los sectores financieros y que se refiere a la necesidad de entender y gestionar posibles problemas o deficiencias asociados a procesos internos, personas, sistemas de información o factores externos. El riesgo operativo (u operacional) actúa como nexo claro y específico entre el Gobierno Corporativo y la gestión estratégica de seguridad, dado que el foco del riesgo operativo no es en absoluto únicamente la tecnología o los riesgos fiduciarios, sino que para poder cubrirlo apropiadamente se debe plantear y actuar también sobre la seguridad de procesos, personas y estructura organizativa.

El fin último de la Gestión Estratégica de Seguridad, en lo tocante al marco de Gobierno Corporativo, es definir y cumplir una serie de requisitos de calidad,

fiduciarios y específicos de seguridad que ayudarán a la organización a alinear sus requisitos de gestión de riesgo con los de negocio, consiguiendo por fin una visión clara y objetiva del valor que aporta fusionar la Gestión de Seguridad con la componente estratégica.

Para poder entender cómo ambos planteamientos se entrelazan se debe tener en cuenta cómo y por qué la gestión estratégica de seguridad aporta valor al Gobierno Corporativo. Dicho valor nace de diversos elementos, como la mejora de la eficiencia operacional, la reducción de costes o el crecimiento de la confianza en la organización. Existen además diversas derivadas a los elementos que aportan valor:

- **Involucrar al negocio en la toma de decisiones relacionadas con la seguridad**. Tal como se comienza a perfilar, uno de los principales factores de éxito es la necesidad de hablar un idioma común, el estratégico, posibilitando que los objetivos de Gestión de Seguridad nazcan de los objetivos de la organización. Si se consigue alcanzar este punto se podrá, por ejemplo, solicitar a las unidades de negocio que participen en la estimación del impacto de un riesgo, lo que además de ofrecer una visión real de cómo éste afecta a la organización como un todo, facilitará que dichas unidades comprendan y hagan suyo dicho riesgo.

- **Potenciar la transparencia, y como primera herramienta, las auditorías**, disciplina a la que este libro dedica un capítulo. Pueden ser de cumplimiento, legales o voluntarias, y aunque las motivaciones para la realización de las mismas pueden ser diversas, su objetivo siempre es la valoración y el control, por parte de un órgano independiente de la adecuación de un proceso a un estándar (sea una legislación, una política interna o una buena práctica). Su fin último es ofrecer confianza a accionistas, clientes, entidades constituidas u órganos de gobierno de la entidad.

- **Aportar información de Gestión de Seguridad**, en contraposición con la carencia endémica de información que han venido sufriendo las áreas de dirección en lo tocante a éste área. Aunque no se trata en absoluto de un problema nuevo, la **medición** de la Gestión de Seguridad se ha convertido en requisito de las pujantes normas y códigos de buenas prácticas, y por tanto, en elemento clave para una correcta conexión entre la estrategia del Gobierno Corporativo y la seguridad, debiendo determinados

indicadores de los Cuadros de Mando de Seguridad formar parte inequívoca de los Cuadros de Mando de la alta dirección. Para ello, dichos indicadores deben estructurarse en diferentes niveles:

- **Negocio**: definen lo que el negocio espera de la Estrategia de Seguridad TI.

- **Dirección IT**: definen qué se espera de los servicios para permitir alcanzar los objetivos de TI en seguridad.

- **Servicio**: miden el rendimiento de los procesos (para indicar si los objetivos van a cumplirse o no).

- **Proceso**: indicadores específicos de rendimiento del proceso, operacionales.

- **Automatización de los procesos IT**, consecuencia directa de la necesidad de medir y gestionar de forma sencilla entornos complejos. En este escenario, la tradicional aproximación artesanal a la operación de las diversas facetas que conforman la Gestión de Seguridad (gestión de riesgos, control del Plan Director, Cuadros de Mando) no puede ser adoptada, debiendo tender hacia la automatización soportada por herramientas apropiadas.

- **Controles orientados al negocio**, enlazados con él y planteados basándose en los activos en los que se apoyan los procesos de negocio y servicios de la organización. Aunque fácil de plantear, esta aproximación supone un esfuerzo importante de interiorización, dado que requiere un replanteamiento del enfoque clásico y pasando a centrarse en el papel de cada activo en la cadena de valor de la empresa.

Afortunadamente para guiar esta transición existen diversas metodologías y buenas prácticas, que abarcan desde el Gobierno Corporativo TI a la Gestión de Servicios.

Una de las metodologías de mayor implantación en lo tocante a Gobierno Corporativo de TI es COBIT, el modelo para el Gobierno de la TI desarrollado por la Information Systems Audit and Control Association (ISACA) y el IT Governance Institute (ITGI). Independientemente de la realidad tecnológica

Ilustración 2.- El papel del Gobierno de Seguridad en la estrategia global.

de cada caso concreto, COBIT determina, con el respaldo de las principales normas técnicas internacionales, un conjunto de mejores prácticas para la seguridad, la calidad, la eficacia y la eficiencia en TI que son necesarias para alinear TI con el negocio, identificar riesgos, entregar valor al negocio, gestionar recursos y medir el desempeño, el cumplimiento de metas y el nivel de madurez de los procesos de la organización.

Sin duda, por su relevancia y popularidad es necesario mencionar el conjunto de buenas prácticas propuestas en ITIL, que aunque en diversos entornos se asocian al Gobierno Corporativo, formalmente no se sitúan en esa capa, sino que pertenecen más propiamente al nivel de Gestión de Servicios TI. ITIL es parte nuclear de la norma ISO 20000 de Gestión de Servicios, a la que se dedicará más adelante un breve capítulo, y que propone una serie de procesos formales que permitirán gestionar los servicios de forma más óptima y, sobre todo, más eficiente y controlada.

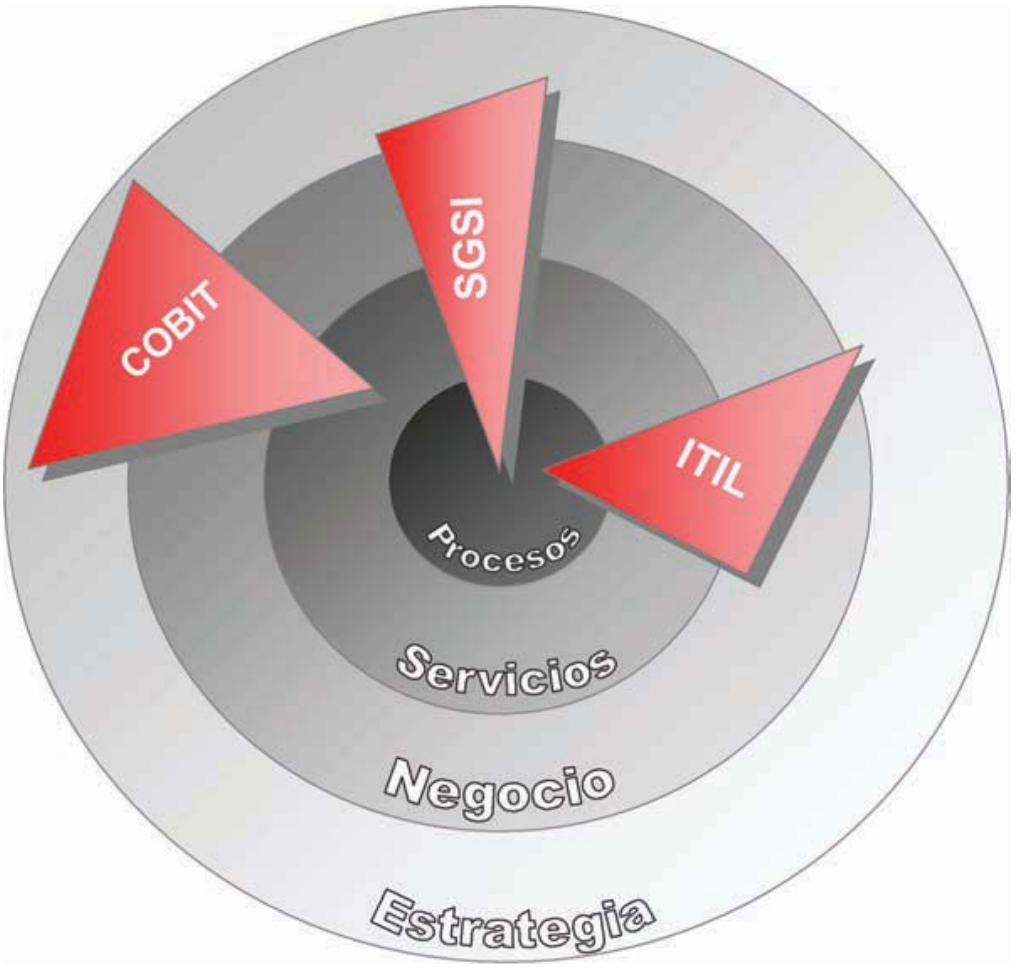

Ilustración 3.- Dominios de las diferentes estrategias de Gestión.

El marco certificable que recoge de forma más global los requisitos y procesos para dotar a la organización de una buena Gestión de Seguridad es el de los Sistemas de Gestión de Seguridad de la Información (SGSI o ISMS en inglés). El planteamiento de los SGSI se traducen en diversas normas que se superponen, dependiendo de su ámbito y foco y que serán enumeradas más adelante, pero cuyo máximo exponente es la internacional ISO 27001, cuya implementación española es la norma UNE 71502.

Un SGSI define una serie de procesos de gestión, alineados con el Gobierno Corporativo de la organización, y un marco de selección de controles (actualmente recogido en la norma ISO 17799:2005) que abarca las principales áreas que deben ser supervisadas en la entidad (normativas, organización, recur-

sos humanos, tecnología, continuidad, cumplimiento legal y regulatorio…). Este conjunto de procesos de gestión será el hilo conductor del presente libro, aunque en diversos puntos se hará referencia a otras metodologías que traten de forma más específica algún área (como la norma BS25999 para la Gestión de la Continuidad de Negocio).

En cualquier caso, afortunadamente y dado el laberinto de normas descritas con anterioridad, existen elementos comunes en todas las metodologías indicadas, lo que permite que sea factible disponer de cierta trazabilidad entre ellas. Esta trazabilidad permite entre otros que, si en algún momento se decide trabajar o complementar unas normas con otras, se puedan "convalidar" procesos entre los diferentes marcos.

Como conclusión, aquella organización que consiga alinear su Gestión de Seguridad con el negocio y plantee ésta basándose en la mejora continua, aunque quizás no perfecta, será capaz de entender sus debilidades y planificar las acciones apropiadas para cubrirlas de forma acorde a sus necesidades, no al mercado, caprichos o requerimientos puntuales.

2. Planificación de la seguridad

◆ 2.1. Estableciendo los cimientos de la estrategia: la política de seguridad y la organización

La planificación de la Seguridad de Información, verdadero corazón de una buena gestión estratégica, formalmente se define como la combinación de políticas, operaciones y estructuras organizativas que buscan asegurar que los planteamientos en Seguridad de la Información están alineados con los objetivos del negocio y son consistentes con las leyes y regulaciones aplicables.

Partiendo de esta ampulosa definición, la realidad tangible y de la que partir es que, como organización, será necesario dar respuesta no sólo a problemas de índole técnica sino que, en muchos casos, los incidentes de mayor relevancia se deben a debilidades o puntos mejorables en la organización (desde defectos de control en procesos a la incorrecta supervisión del personal de limpieza).

¿Qué es entonces la Política de Seguridad? Existen varias definiciones, atendiendo a la visión o alcance estratégico, pero que en el plano más tangible no es ni más ni menos que un conjunto de documentos, con un orden y una sistematización determinados, que indican las normas, procedimientos y actuaciones que se deben cumplir en la entidad.

Sin embargo, ahondando en el concepto y ubicando la definición en el plano de la estrategia (donde a partir de ahora se deben mover las reflexiones del responsable de seguridad), la Política de Seguridad es un instrumento que desarrolla los objetivos de seguridad de la organización a largo plazo, siguiendo un ciclo de vida (desde su definición hasta la implementación y revisión posterior), y deberá ser la base a partir de la cual se diseñe el sistema de seguridad. Para ello, es absolutamente imprescindible que la alta direc-

ción haga suya dicha política, la firme y establezca la obligatoriedad de su cumplimiento. Esto garantizará una apropiada consideración y compromiso por parte de la organización, factor clave para su éxito.

Algunos de los atributos más relevantes que ayudarán a poner en contexto la Política de Seguridad son:

- La Política de Seguridad y cuerpo normativo adjunto establecen formalmente qué se puede hacer y qué no, no quedando sólo un conjunto vago de recomendaciones tornadizas.

- Si está apropiadamente organizada y recoge fehacientemente los objetivos de la organización, será una excelente base sobre la que tomar las decisiones en materia de inversiones en seguridad.

- Demuestra un compromiso de la dirección de la entidad con la seguridad.

- Su presencia y aprobación es uno de los elementos estructurales de las principales normativas y estándares de seguridad, no siendo en ningún caso opcional o accesoria.

- La Política de Seguridad y normativas asociadas son un elemento extremadamente útil frente a las auditorias de cumplimiento, dado que ofrece una lista clara de los elementos a comprobar, ofreciendo en consecuencia resultados útiles y objetivos, no basados en parámetros de valoración ajenos a la organización.

Aunque no existe una definición formal, clara y ampliamente aceptada de los diversos componentes del cuerpo normativo de seguridad, una de los desarrollos documentales más coherentes es el que se describe en este esquema.

Ilustración 4.- Estructura del cuerpo normativo.

- **Política**: objetivos a alto nivel de la organización, compromiso de dirección y su obligatoriedad.

- **Normativas**: desarrollo de la política para campos concretos del alcance (personal, seguridad física, comunicaciones…).

- **Procedimientos**: cómo aplicar la normativa en los activos concretos de la organización.

Es de vital importancia entender que la política de seguridad y sus normativas asociadas no son elementos estáticos e impermutables, sino un conjunto vivo de directivas que deben evolucionar junto con la organización. Para ello, será necesario definir un ciclo de vida, que aunque por simplicidad se plasma en una lista ordenada no es un proceso secuencial, y que a alto nivel podría ser:

1. Definición del equipo de redacción y de aprobación.
2. Desarrollar la política general.
3. Definición de la estructura.
4. Análisis de la integración con otras normas.
5. Definición de los temas de seguridad a incluir en normativa.
6. Definición del esquema de cada documento.
7. Desarrollar las normas.
8. Desarrollar los procedimientos.
9. Desarrollar las instrucciones de trabajo.
10. Aprobar el contenido en sus distintos niveles.
11. Definir el método de difusión y mantenimiento permanente.
12. Definir el método de "premios y castigos".
13. Implementar la normativa.
14. Ejecutar los mecanismos de actualización.

Como resalte, es importante destacar que la aprobación de la Política de Seguridad y de su cuerpo normativo asociado es uno de los puntos más complejos dentro del ciclo de vida de la misma, dado que implica la necesidad de alcanzar un consenso entre todos los implicados en su redacción. Esta aprobación además suele aflorar derivadas no contempladas, como por ejemplo la dificultad de que alta dirección preste su apoyo en algo que, si no se ha transmitido apropiadamente, puede ser percibido como "inhabilitación" de los procesos productivos o de negocio.

La estructura y papel de las áreas de Seguridad de la Información también está sufriendo una evolución paralela a este proceso de madurez, similar a la experimentada por las áreas de Recursos Humanos, que comenzaron como áreas de "Personal" adscritas a Apdos. Financieros (personal como coste), actualmente son generalmente denominadas "Recursos Humanos" (personal como recurso), existiendo una clara tendencia hacia la evolución a áreas de "Capital Humano" (personal como activo que aporta valor).

De esta forma, aunque la seguridad ha sido históricamente adscrita a las áreas de informática o TI, se está observando una tendencia creciente a situarla como un área de staff, en dependencia directa de la alta dirección, similar a las de Calidad o Recursos Humanos y cuya función es horizontal a toda la organización (dado que desde su nicho dentro de TI le ofrecía

una visión muy limitada del negocio y una capacidad de actuación más reducida aún sobre áreas diferentes a TI).

Este nuevo papel no infiere automáticamente en que las habilidades del personal de Gestión de Seguridad vayan a ser compatibles con su nueva posición, sino que representará una importante dosis de esfuerzo para la Dirección de Seguridad tradicional. Este nuevo responsable deberá contar con nuevas habilidades y capacidades, acordes a sus nuevas responsabilidades e imprescindibles para una relación armoniosa con otras áreas con las que deberá tratar y hacer partícipes de su estrategia, como Calidad, Dirección o *Marketing*.

Para conseguir la máxima integración de los objetivos de negocio con los de seguridad es muy recomendable el establecimiento de un Comité de Seguridad, cuya principal función será la toma de decisiones y gestión continuada en todo lo tocante a la Seguridad de la Información, debiendo constituirse como el órgano de gestión máximo en esta materia. Sus funciones y relevancia se tratan de forma específica en diversas normas, especialmente en la ISO 17799:2005, por lo que, en mor de la brevedad, se recomienda al lector acudir a esta fuentes para ampliar información.

Resumiendo de forma simplista la transición organizativa descrita previamente, el papel que deberá desempeñar el responsable de seguridad estará condicionado en gran medida por sí mismo y su capacidad, convirtiéndose en un director en el que se confía, implicado en las decisiones de negocio, o en un gestor técnico cuya labor es "mantener las luces encendidas y funcionando lo más barato posible".

◆ 2.2. Gestión del riesgo: ¿Cuánto cuesta la seguridad?

Cualquier organización que se enfrente a la problemática de proteger sus activos de información debe responder dos preguntas:

- **¿qué seguridad necesito?**
- **¿cuánto me cuesta la seguridad?**

A la primera de estas preguntas se responde a través de un trabajo de análisis en el cual la organización reflexiona sobre la importancia de sus activos de información y evalúa los requisitos de seguridad que ha de satisfacer.

A la segunda de las preguntas se responde identificando los medios que la organización ha de disponer para cumplir sus requisitos de seguridad y evaluando el coste de los mismos.

La principal dificultad a la que se enfrentará la organización a la hora de desarrollar estos trabajos será disponer de un modelo de referencia que le permita "medir" la seguridad requerida y evaluar el coste asociado.

En la actualidad es posible identificar dos tendencias o modelos de referencia significativos:

- Modelos basados en buenas prácticas o controles generales.
- Modelos basados en análisis y gestión de riesgos.

Los primeros de estos modelos se basan en clasificar los activos de información por niveles de seguridad y establecer los controles o medidas de seguridad que deben aplicarse a cada nivel definido. Estos modelos reducen la complejidad en el tratamiento de los requisitos de seguridad y establecen un modelo de gestión sencillo.

Los segundos de estos modelos se basan en la definición del concepto de riesgo como medida de la seguridad. El concepto de riesgo puede representarse tal y como se muestra en la siguiente ilustración.

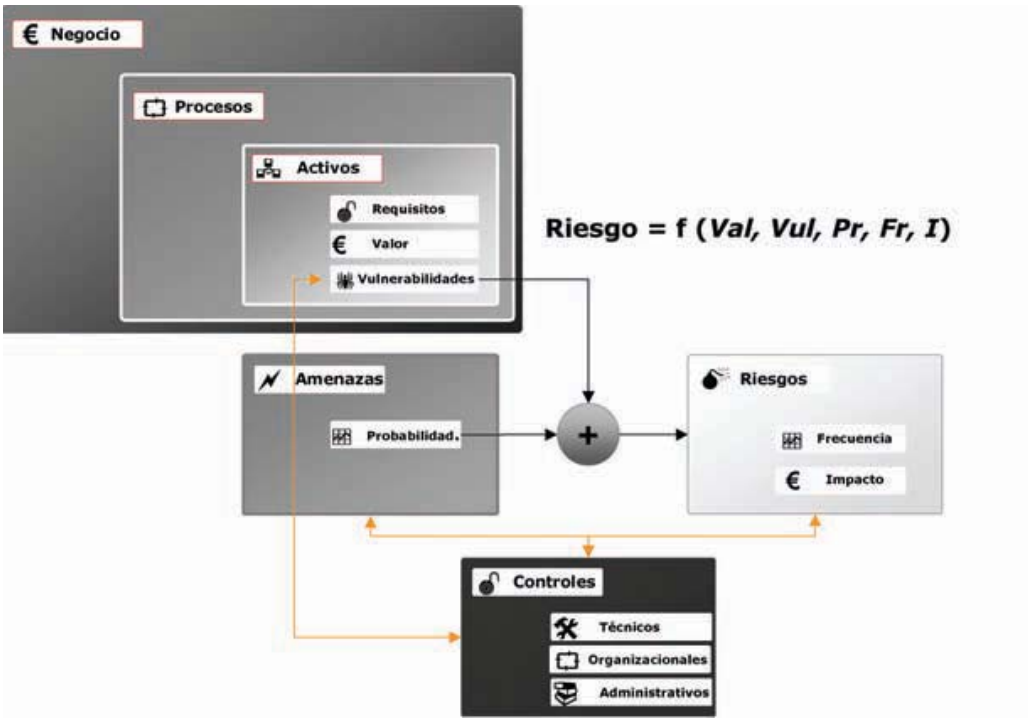

Ilustración 5.- Modelo del Riesgo.

Desde la perspectiva de los modelos basados en el análisis y gestión de riesgos, los activos de información de la organización están sujetos a un conjunto de amenazas internas y externas que pueden hacer uso de vulnerabilidades presentes en los activos para ocasionar incidentes de seguridad. Estos incidentes producirán una degradación o impacto en los activos de información y, por ende, en los procesos y servicios de negocio.

Con el fin de evitar dichos incidentes, la organización debe desplegar un conjunto de controles de seguridad.

El riesgo se define pues como una función de los activos, las vulnerabilidades, las amenazas y los posibles impactos sobre los procesos y servicios de negocio.

El modelo de análisis y gestión de riesgos se postula como una sólida alternativa para la Gestión de la Seguridad en la organización. Su relevancia está avalada por el desarrollo de numerosos estándares nacionales e internaciona-

les (ISO, NIST, etc.), así como en el desarrollo de numerosas metodologías y herramientas que los implementan (MAGERIT, CRAMM, Octave, etc.)

El proceso de análisis y gestión de riesgo propuesto por estos estándares puede resumirse en los siguientes pasos:

- **Establecimiento del alcance del análisi**s, identificando los activos de información que deban ser contemplados.

- **Identificación de los riesgos**. Identificación de las vulnerabilidades y amenazas a las que están sujetos los activos de información comprendidos en el alcance.

- **Análisis de los riesgos**. Valoración de los riesgos identificados, en función de su probabilidad de ocurrencia e impacto asociado.

- **Evaluación de los riesgos**. A partir del análisis de riesgo, la organización procede a evaluar los mismos y decidir si son asumibles o no. En caso de no serlos, se procederá a tratar los mismos.

- **Tratamiento de los riesgos**. Despliegue de controles y contramedidas de seguridad que mitiguen los riesgos.

2.2.1. Identificación de activos: el corazón del negocio

El objetivo de toda Estrategia de Seguridad de la Información es proteger los activos de información de la organización. Y la razón para ello es la dependencia entre los servicios y procesos de negocio de una organización y dichos activos.

Hoy por hoy, cualquier actividad, servicio o proceso de negocio desarrollado por una organización depende, en mayor o menor medida, de la información y los medios empleados para su procesamiento, almacenamiento o trasmisión. Cualquier disrupción en estos últimos supone un impacto en las actividades de la organización.

Como se ha comentado con anterioridad, el modelo de análisis y gestión de riesgos persigue identificar los riesgos a los que se encuentran sometidos los

activos de información, de forma que la organización pueda priorizar los mismos y adoptar las medidas adecuadas.

Por lo tanto, el primer paso que debe plantearse toda organización es conocer cuáles son sus activos de información y cómo sus servicios y procesos de negocio se apoyan en los mismos.

A tal fin, la organización debe abordar un proceso de inventariado de activos de información. Este proceso debe seguir una aproximación de arriba a abajo (*top down*), identificando en primer lugar los servicios proporcionados por la organización. A continuación, se debe proceder a identificar los procesos de negocio implicados para, finalmente, identificar los activos de información que dan soporte a dichos procesos. De esta forma, la organización dispondrá de un inventario o mapa de activos sobre el cual desarrollar el posterior análisis de riesgos.

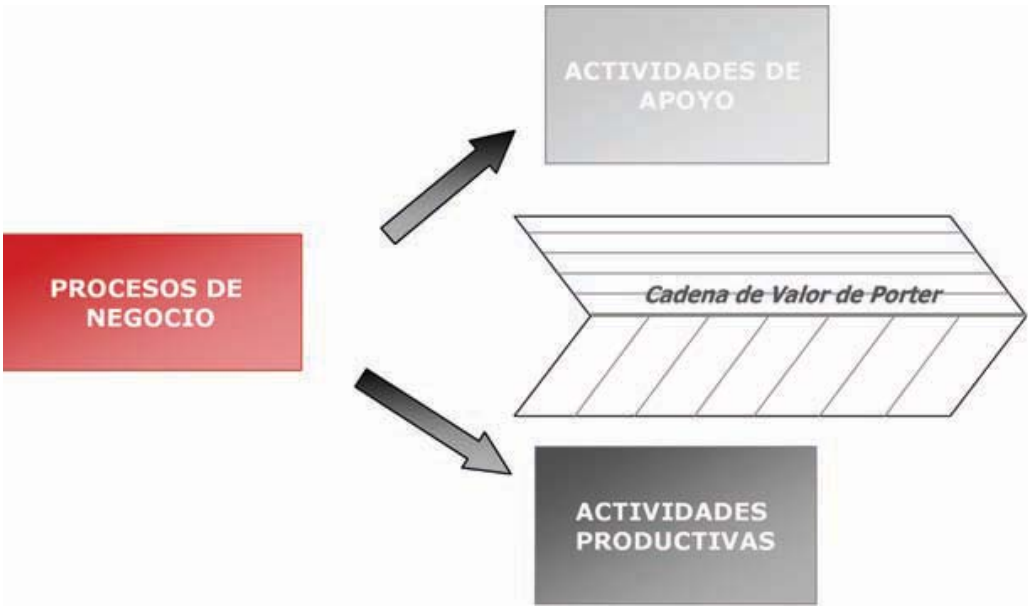

Ilustración 6.- De los servicios a los activos.

Es importante resaltar que no sólo interesa disponer de una enumeración de servicios, procesos y activos, si no que resulta indispensable conocer las relaciones y dependencias existentes entre los mismos.

¿Por qué incluir en un inventario de activos los servicios y procesos de negocio de la organización? El modelo de análisis y gestión de riesgos es capaz de identificar las amenazas y vulnerabilidades a las que se encuentran sometidos los activos de información. En caso de materializarse una determinada amenaza en forma de un incidente de seguridad, el impacto tendrá una doble vertiente:

- En primer lugar, afectará al propio activo de información, en forma de degradación o pérdida del mismo.

- En segundo lugar, la degradación o pérdida de un activo afectará a los procesos de negocio que lo utilizaban y, por ende, a los servicios proporcionados por la organización.

Es decir, las amenazas se materializan, explotando las vulnerabilidades, en los activos de información, mientras que el impacto repercute en los servicios y procesos de negocio.

Un enfoque alternativo es pensar que los activos de información tienen asociado un determinado valor. ¿De qué depende el valor de un activo? Fundamentalmente de su importancia desde la perspectiva de los servicios y procesos de negocio de la organización. Así, un activo de escasa relevancia desde la perspectiva de los procesos de negocio tiene poco valor para la organización.

2.2.2. Amenazas de seguridad y vulnerabilidades

Establecido el mapa o inventario de activos de información de la organización, el análisis de riesgos prosigue con la identificación de las amenazas y vulnerabilidades.

Por amenaza debe entenderse cualquier escenario o situación que potencialmente puede materializarse como un incidente de seguridad. El abanico de amenazas al que se encuentra sometido el inventario o mapa de activos de la organización es variado:

- Desastres naturales: terremotos, huracanes, etc.
- Siniestros: inundaciones, incendios, etc.
- Accidentes.

- Agresiones.
- Etc.

Toda organización debe elaborar una lista exhaustiva de las amenazas a las que pueda estar sometida para, posteriormente, evaluar la probabilidad de que dicha amenaza se materialice sobre los activos de información.

Por ejemplo, al considerar como posible amenaza un terremoto, la organización debe analizar la probabilidad de ocurrencia a partir de los informes de actividad sísmica de la zona en la que se ubiquen los activos de información en cuestión.

En ocasiones, como el caso de la amenaza por terremoto, la probabilidad puede calcularse a partir de información estadística existente. En otras ocasiones, esto no será posible, por lo que tendremos que recurrir a estimaciones y aproximación.

A la hora de estimar la probabilidad de materialización de una amenaza, es necesario tener en consideración si el activo de información es vulnerable o no ante dicha amenaza.

Veámoslo con un ejemplo: el virus del sarampión. ¿Cuál será la probabilidad de materialización de esta amenaza? Pues dependerá de si nos hemos vacunado o no contra dicho virus. Toda persona vacunada contra el virus del sarampión será inmune a dicho virus, es decir, no será vulnerable ante el virus. La probabilidad de contraer el virus es cero. Sin embargo, una persona que no haya sido vacunada contra el virus tendrá una cierta probabilidad, mayor que cero, de contraer la enfermedad.

En el caso de las amenazas y activos de información, estamos ante el mismo caso. La pregunta a hacerse para estimar la probabilidad de materialización es, en primer lugar, si el activo es o no vulnerable ante determinada amenaza.

Existen amenazas ante las cuales todos lo activos son vulnerables: desastres, siniestros y accidentes. Existen otras antes las cuales, dependiendo de las medidas y controles de seguridad adoptados por la organización, se puede o no ser vulnerable: las agresiones y actos intencionados.

2.2.3. El riesgo como factor de la seguridad

Como ya se ha anticipado en un capítulo anterior el concepto de riesgo permite definir un marco de referencia para evaluar la seguridad de la información.

El proceso de evaluación y valoración del riesgo permite a la organización determinar el grado de exposición de sus activos y definir una estrategia orientada a reducir la misma.

Mediante el despliegue de controles de seguridad, la organización puede actuar sobre los factores del riesgo, mitigando las vulnerabilidades, reduciendo la probabilidad de materialización de una amenaza o minimizando el impacto sobre los activos en caso de producirse un incidente de seguridad.

La siguiente ilustración muestra cómo evoluciona el riesgo.

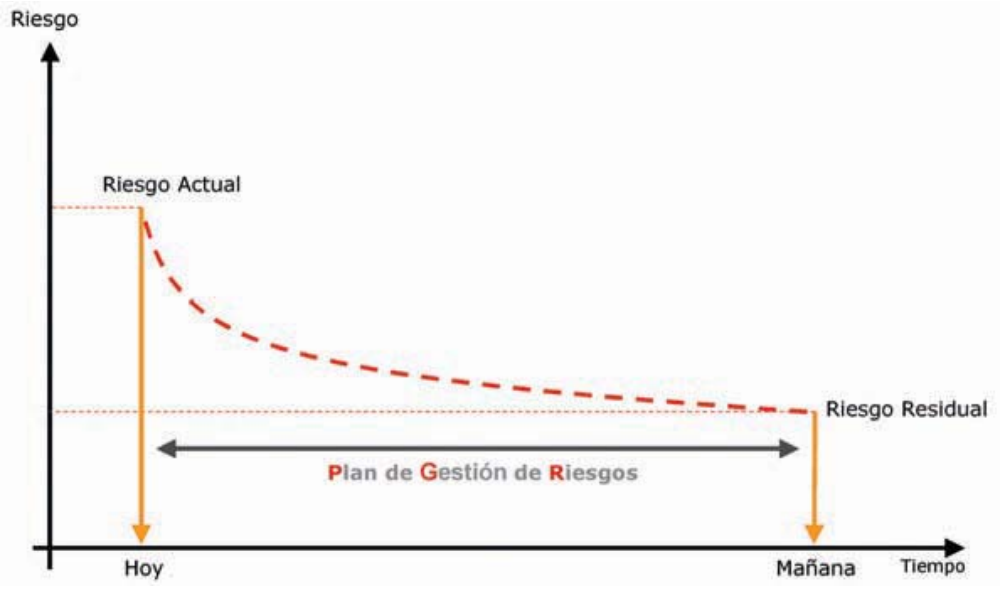

Ilustración 7.- El Plan de Gestión de Riesgos.

La definición y ejecución de un Plan de Gestión de Riesgos permitirá a la organización alcanzar un nivel óptimo de seguridad definido por un riesgo residual. Este riesgo residual comprende el conjunto de riesgos que la organización considera asumible, bien porque la probabilidad de ocurrencia es baja o porque el impacto es desdeñable.

La definición de este umbral de riesgo residual es una decisión que estará relacionada con la aversión al riesgo de la organización.

Finalmente, es necesario reflexionar sobre la necesidad de desplegar un proceso de monitorización continua del riesgo. Ciertamente, el entorno dinámico en el que se encuentran las organizaciones obliga a las mismas a realizar cambios continuos para adaptarse. Estos cambios se producen a distintos niveles y en distintos entornos: reorganizaciones, fusiones y adquisiciones, crecimiento, etc. Todos estos cambios afectan al perfil de riesgo de la organización.

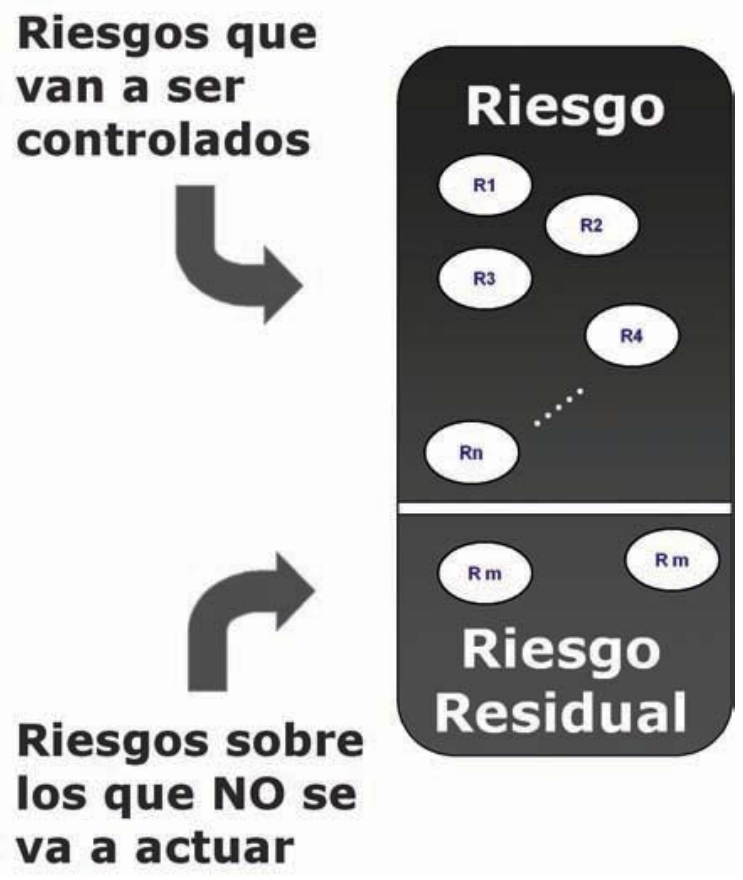

Ilustración 8.- El concepto del umbral de riesgos.

Dicho de otra forma, el riesgo al que se encuentra sometida la organación es variable y, desgraciadamente, con una clara tendencia creciente. En consecuencia, el proceso de evaluación y valoración de riesgos debe ser un proceso continuo para adaptar la estrategia de seguridad de la organización y ubicar a la misma en el umbral de riesgo residual requerido.

2.2.4. Algunas realidades en la Gestión del Riesgo

Lo cierto es que toda la teoría expuesta en los capítulos anteriores es aplicable y de gran utilidad. Sin embargo, tal y como se suele decir, de lo dicho al hecho hay un gran trecho.

Más aún, una buena cantidad de años en el sector deja claras algunas realidades. Entre ellas, que hay multitud de entidades que desconocen lo que tienen, para qué lo usan, quiénes lo usan, y quiénes lo deberían usar. Generalmente, el problema es más acuciante cuanto mayor es la entidad y más compleja su organización.

Si una entidad no sabe qué activos componen sus sistemas de información, difícilmente podrá abordar un análisis de riesgos. Obviamente, si una entidad no sabe qué activos tiene será incapaz de determinar su valor, sus vulnerabilidades y las amenazas a las que se encuentra expuesta.

En mayor o menor medida las responsabilidades, los presupuestos y los activos se encuentran generalmente diluidos en la organización. De este modo, cada unidad o departamento es razonablemente consciente de los activos que utiliza para la explotación de sus procesos. Sin embargo, en general es desconocedor de los activos de soporte. Como es de esperar, exactamente lo opuesto suele ocurrir en los departamentos de sistemas y comunicaciones.

Similarmente, es complicado determinar la valoración intangible de los activos de una organización y mantenerlos razonablemente actualizados. Por ejemplo, una entidad puede determinar que su imagen es un activo muy importante o incluso crítico; sin embargo, valorar la imagen no es algo obvio, y mucho menos determinar cómo los activos de los sistemas de información afectan a la misma.

Posiblemente, después del cumplimiento de requisitos legales, la característica de la seguridad de los sistemas de información más fácil de justificar sea la disponibilidad. ¿Cuánto dinero pierdes si no tienes disponible durante 24 horas el servicio? La respuesta a esta pregunta suele ser inmediata cuando te contesta el responsable de una unidad que a su vez es un centro de beneficios.

Por el contrario, qué ocurre cuando le haces esta pregunta al responsable de sistemas sobre el servicio de correo electrónico o navegación en Internet. En estos casos, lo habitual es que el responsable de sistemas conteste que no lo sabe; sin embargo, es capaz de asegurar el alto número de incidencias y/o el número de coscorrones que le llegarían.

Obviamente, si se hablase sobre aspectos relacionados con la confidencialidad o integridad, las discrepancias o la complejidad serían aún mayores.

Aun contemplando únicamente la característica de disponibilidad, es complicado patrocinar la implantación de salvaguardas globales. Puesto que influyen a la totalidad de la entidad, estos análisis y selección de contramedidas deben ser patrocinados y financiados desde los estamentos más altos de la organización.

Adicionalmente, los requisitos de seguridad son bastante particulares según el sector y relativamente dinámicos. Consecuentemente, puesto que uno de los aspectos de mayor consideración a la hora de cuantificar el riesgo es la valoración del activo o del impacto. Algo que antes era considerado de bajo riesgo puede haber evolucionado hasta considerarse en la actualidad como crítico. Con el fin de evitar falsas sensaciones de seguridad es importante mantenerlo actualizado.

Paralelamente, a la hora de abordar un análisis de riesgos es fácil caer en la tentación de considerar la disponibilidad como la característica principal de la seguridad. La disponibilidad es un concepto que prácticamente todos conocen, que han sufrido en alguna ocasión y que fácilmente es asociado a pérdidas. Seguro que para muchas entidades la disponibilidad de sus sistemas es la piedra filosofal; sin embargo, teóricamente hablando es cuestionable abordar el Plan de Continuidad de un CPD valorado en 10 millones de euros con un 0,1% de probabilidad de que un desastre natural lo inutilice. A menos, claro está, que dicho CDP dé soporte al negocio de una cantidad nada despreciable de euros anuales.

Tal y como se ha mencionado con anterioridad, la valoración del riesgo relacionado con la disponibilidad de los sistemas de información es relativamente sencilla. Sin embargo, ¿Qué ocurre cuando se tratan las otras dos dimensiones de la seguridad?

Cuando se aborda la determinación del impacto relacionado con la confidencialidad y/o integridad, la valoración se complica más aún. Cuánto vale la información que tiene una entidad o qué impacto supone su revelación pública. Esta pregunta me la formuló en su momento un cliente, lo cierto es que es una pregunta bastante complicada. Sin embargo, la respuesta formulada a la gallega fue prácticamente inmediata. En el supuesto caso de que pudieseis, y que esto no fuese ilícito, cuánto estaría dispuesto a pagar vuestro departamento comercial por disponer de esa misma información de vuestra feroz competencia.

Pensemos en un gran banco y en lo que le sucedería si sus sistemas no estuviesen disponibles durante 9 horas laborables. Posiblemente las pérdidas serían considerables. Ahora, valoremos la posibilidad de que toda la información relacionada con sus clientes fuese repentinamente publicada en medios alternativos, posiblemente el banco las pasaría canutas. Por último, pensemos que todos los datos de sus clientes y que las transacciones realizadas durante el último mes fuesen erróneas. Lo cierto es que es difícil escoger joyas entre estas posibilidades. Sin embargo, si se le pregunta a un banco o se analizan los escenarios propuestos, posiblemente se concluirá que los impactos son importantes, pero que la probabilidad de ocurrencia no es la misma.

Como entidad privada, un banco puede tener más o menos clara la valoración de su información. Sin embargo, siendo aún más quisquilloso, cómo se valorarían los riesgos enumerados en los tres escenarios anteriores en una Administración Pública. Qué ocurriría si esto le sucediese a la Agencia Tributaria.

Básicamente, estos son los ejercicios que hay que realizar a la hora de abordar un análisis de riesgos de los sistemas de información. Obviamente, es complejo determinar el impacto económico en cualquiera de los casos. Sin embargo, es relativamente sencillo llevar a cabo estudios cualitativos basados en las premisas enumeradas en los capítulos anteriores.

En cualquier caso, a la hora de abordar un análisis de riesgos hay que tener tres consideraciones adicionales. La primera consideración es ser metódico para poder realizar el análisis tantas veces como sea necesario a lo largo del tiempo. La segunda consideración es ser realista, el análisis de riesgos será tan bueno como la información disponible. Adicionalmente, hay que ser riguroso, y justificar los impactos. Para los responsables de servicios, los suyos son siempre los más críticos.

Realmente, los objetivos fundamentales de un análisis de riesgos son conocer mejor los sistemas de información y sus dependencias con el negocio, y poder establecer las contramedidas apropiadas acorde al nivel de riesgo que se está dispuesto a aceptar.

En consecuencia, la Gestión del Riesgo deberá incluir por un lado el propio análisis de riesgos, idealmente actualizado, y por otro una planificación de acciones, tareas y proyectos que permitan a la Entidad alcanzar y mantener el nivel de riesgo que está dispuesto a asumir.

De este modo, se parte del riesgo intrínseco, que equivale al riesgo de una entidad sin la implantación de contramedidas, y, conforme se van aplicando las contramedidas se podrá ir viendo cómo el riesgo efectivo disminuye.

Obviamente, para gestionar el riesgo se implantarán distintos tipos de medidas que debieran disminuirlo. De este modo, existirán medidas técnicas, documentales, procedimentales, funcionales, etc.

Al final, lo importante es sentirse razonablemente a gusto con el resultado del análisis de riesgos. Dicho análisis siempre será mejorable, se podrá entrar en mayor detalle. Se podrán incluir nuevas funcionalidades e incluso valoraciones económicas. Sin embargo, en la elaboración del primer análisis de riesgos es aconsejable delimitar el alcance y evitar en gran medida el detalle.

De hecho, el propio análisis nos indicará aquellos aspectos sobre los que se deberá profundizar. Del mismo modo, si a la hora de realizar el análisis de riesgos no se encuentra algo sorprendente, puede ser porque se conozca demasiado bien el negocio o porque no se haya realizado con la rigurosidad oportuna.

Si por el contrario, uno se encuentra con que la práctica totalidad de activos de los sistemas de información tienen consideración muy crítica para las tres dimensiones de seguridad, es que no se ha entendido correctamente el espíritu del propio análisis o que se tiene un gran desconocimiento del negocio.

En sí, abordar la realización de un análisis de riesgos es una experiencia enriquecedora y si hay una participación generalizada por parte de la entidad puede ser una actividad divertida. En cualquiera de los casos, el resultado de

dicho análisis debe ser validado por una persona de peso en la organización. Generalmente, él dará una visión adicional sobre la criticidad de los distintos procesos que componen el negocio.

◆ 2.3. Abordando de forma práctica la planificación de la seguridad en la empresa: el Plan Director de Seguridad

Como ya se ha expuesto anteriormente, la gestión de riesgos es la verdadera piedra angular y punto de partida de todas las iniciativas de Gestión de la Seguridad, y permite conocer cuáles son las prioridades reales de protección. Como dice la máxima… "Si no sabes dónde estás, ¿para qué quieres un mapa?"

En este punto, la organización no sólo intuye cuál es el verdadero corazón de su negocio, sino que ha conseguido identificar los activos más relevantes que soportan sus procesos, y conoce las relaciones y dependencias que existen entre ellos, configurando un mapa de activos y sistemas. La entidad entiende los puntos débiles de los que adolecen los activos (tanto solos como en conjunto), y el impacto de las amenazas que pueden materializarse sobre ellos. Este camino de reflexión y análisis interno, que ha servido para valorar el riesgo al que se enfrenta la organización, habrá conseguido además concienciar tanto a los sectores técnicos como a los de negocio acerca del papel que ejerce la seguridad en la estrategia de la compañía. Sin embargo, a pesar de que el Análisis de Riesgos es un proceso extremadamente útil que permite comprender mejor las necesidades de la organización, está anclado al momento temporal en el que se realiza. En contraposición, el objetivo perseguido por la organización debe ser dinámico y adaptable, y debe permitir gestionar la seguridad desde el plano estratégico.

El Plan Director de Seguridad, o Plan de Seguridad, supone el desarrollo de los objetivos estratégicos identificados en la política y normativas de seguridad de la organización, y su finalidad es ubicar a la entidad, a nivel global, en un entorno de riesgo aceptable. En la práctica es una herramienta sistemática que permite establecer pautas y directrices para planificar de forma ágil las diferentes iniciativas que la organización, hasta ese punto, había abordado de forma aislada y parcial. Hilando esta definición con el aforismo que ha abierto el capítulo, el Plan Director de Seguridad es el camino, que se refleja en el mapa, que sirve para guiar los pasos de la organización en el cumplimiento de sus objetivos de seguridad.

Recapitulando, los pasos que la Entidad ha recorrido en la senda hacia la Gestión Estratégica de Seguridad son:

- Diseño, redacción y aprobación de la Política de Seguridad de la organización. Este documento desgrana los objetivos estratégicos de la entidad en materia de seguridad, y plantea el alcance de los mismos.

- Análisis de Riesgos de los procesos incluidos en el alcance de la Política de Seguridad. Gracias a él, se conocen los activos que soportan los procesos (conocimiento del entorno), así como las vulnerabilidades de las que adolecen y las amenazas a las que se enfrentan.

En este punto, el objetivo es identificar y planificar las acciones, correctivas o de mejora que permitirán reducir los riesgos identificados para los activos, y luego plasmarlas y gestionarlas a través del Plan Director de Seguridad. Muchos de los riesgos podrán ser reducidos mediante la aplicación de un único control de baja complejidad (como por ejemplo, la implantación de un sencillo antivirus). No obstante, en numerosas situaciones no bastará con una actividad sencilla y habrá que diseñar proyectos específicos para afrontar riesgos complejos (como el diseño e implantación de un Plan de Contingencias).

El principal sustrato de la elaboración de un Plan Director de Seguridad es una colección de actividades, muchas de ellas con carácter complejo, que se deberán abordar para alcanzar el objetivo de seguridad establecido a través del umbral de riesgo. En síntesis, para cubrir cada uno de los riesgos que deben ser controlados a través del Plan Director de Seguridad se proponen un conjunto de líneas de acción, así como proyectos mediante los cuales implementarlas.

Tras disponer de dicha colección de actividades y proyectos derivados, la siguiente incógnita es el orden en el que se deberán acometer. Sin duda, la mejor opción es priorizar las acciones en base a un único criterio maestro, aunque luego se utilizarán otros que matizarán dicha ponderación. El criterio base a la hora de planificar y priorizar el despliegue de los controles de seguridad será el **nivel de riesgo cubierto** por el control. Asociada a cada línea de acción se dimensiona también el beneficio cuantitativo obtenido tras su implementación para cada dimensión de seguridad (confidencialidad/integridad/disponibilidad).

Su objetivo es por tanto priorizar las líneas de acción y definir diferentes **categorías** de proyectos:

- **Inmediatos** (también denominadas *Quickwins*, y que permiten obtener resultados importantes en un tiempo o con unos recursos mínimos).
- **Corto plazo**.
- **Medio plazo** (como máximo 2 ó 3 años)

La adopción del criterio de "largo plazo" en un Plan Director de Seguridad es de escasa aplicación, dada la alta mutabilidad de los riesgos, que evolucionarán de forma muy significativa en un período de tiempo largo.

Ilustración 9.- Visión del Plan de Seguridad.

Una vez definidas y priorizadas en una primera iteración las acciones y proyectos en base al nivel de riesgo cubierto, se deben plantear ciertos subcriterios que servirán para matizar el orden con el que las acciones y proyectos se acometen:

- El primer criterio que se deberá contemplar e intentar maximizar es el de la aplicación de **controles que cubren más de un riesgo**. Aunque por

defecto el orden estricto de aplicación sea el basado en el concepto de riesgo cubierto, es muy recomendable aumentar la prioridad de acciones que cubran múltiples riesgos, y que por tanto, disminuyan el riesgo soportado de forma global.

- Dado que cada una de las líneas de acción que derivan del Plan Director de Seguridad tendrá asociada una serie de costes, es posible seleccionar qué líneas de actuación abordar en función de un **criterio de eficiencia/eficacia/coste**. Este planteamiento es especialmente relevante en los casos que se cumpla por **defecto**, es decir, aquellas iniciativas que, aunque no cubran un riesgo muy significativo, su coste es bajo o inexistente. Es recomendable que dichas iniciativas se ubiquen dentro de las acciones consideradas como quickwins.

- Asimismo, y siguiendo los criterios planteados a lo largo de la obra, es imprescindible tener en cuenta las consideraciones de negocio en cuanto a su aplicabilidad de controles: se debe identificar y determinar qué controles son más relevantes para la organización, especialmente los adyacentes que se ubiquen en el mismo nivel de riesgo cubierto. Un ejemplo práctico es el uso de controles que potencian la imagen o rendimiento de un área específica de la compañía.

Finalmente, es importante hacer notar que, dado que el Plan Director de Seguridad se ubica en el plano de la estrategia, se deben definir ciertos atributos indispensables para cualquier iniciativa que se vaya a planificar:

- **Fecha de comienzo y duración**: cada proyecto derivado del Plan Director de Seguridad, independientemente de su prioridad, debe planificarse en un marco temporal concreto, indicándose así mismo su duración. Es especialmente recomendable mantener de forma paralela a la representación tradicional del Plan Director de Seguridad (apoyada normalmente en hojas de cálculo o herramientas avanzadas) un diagrama de Gantt del proyecto. Gracias a esta representación, será posible entender de forma más clara las dependencias y ejecuciones paralelas de tareas, lo que permitirá a su vez optimizar la planificación.

- **Recursos y presupuesto**: este punto es donde se produce el nexo más importante con el negocio de la organización en el plano financiero. Dado

que a través del Plan Director de Seguridad se planifica la seguridad de forma proactiva y proporcional, a partir de su creación será posible presupuestar y aprovisionar apropiadamente este capítulo. Así mismo, y dada su naturaleza, en muchos casos los conceptos asociados al epígrafe de gastos podrán ser gestionados como inversiones. De forma adicional, este punto debe desgranar el coste económico de cada proyecto o línea de acción en, al menos, materiales, contrataciones externas y personal (se debe contemplar el coste tanto para personal externo como la ocupación interna de recursos).

- **Responsable de proyecto/acción**: toda acción deberá tener un único responsable cuya función principal en el marco del Plan Director será controlar que dicha tarea se inicia en el momento que debe y cumple la planificación propuesta. Ante desvíos sobre lo esperado, ya sea en el plano temporal, de recursos o presupuestario, éste deberá informar inmediatamente para emprender las acciones correctivas pertinentes. Además, una de sus principales funciones será presentar el estado y logros de cada iniciativa al resto de personal involucrado y crear resúmenes ejecutivos para la alta dirección.

- **Nivel de riesgo que cubre**: tal como se ha comentado con anterioridad, éste es el verdadero indicador de prioridad de cada acción y se debería indicar en el Plan Director. Este punto es uno de los principales nexos de unión con la Gestión de Riesgos realizada.

- **Otros**: adicionalmente, se pueden reunir, según el nivel de madurez en la Gestión de Seguridad de la organización, diversos indicadores. Entre ellos, siempre resulta interesante el **ratio coste/beneficio**, las dependencias con otras acciones correctivas y, en caso de que se usen normas ISO para la selección de controles, trazabilidad con los controles de las mismas que cubre cada línea de acción o proyecto.

Una de las principales dificultades detectadas por parte de diversas organizaciones en este campo es la gestión del Plan Director de Seguridad. Estos conflictos, especialmente en organizaciones de cierto tamaño, nacen de la complejidad que supone la implantación de diversos proyectos de un área en la que habitualmente no existe suficiente personal cualificado. Es recomendable el agrupar los proyectos según las áreas de conocimiento para facilitar su control (procesos y servicios, tecnología, seguridad física, legislación o iniciativas mixtas).

Con las prácticas descritas en esta publicación debería resultar más sencillo abordar dicho proceso, dado que en el plano de gestión los conceptos son comunes a los clásicos de la dirección estratégica. Aun así, es vital disponer de asesoramiento experto en las áreas técnicas relacionadas con la seguridad, y asegurarse de que en la definición de los roles y responsabilidades en la compañía se incluyan actividades de planificación en seguridad de la información.

Por otra parte, existe una alternativa a esta metodología de gestión del Plan Director de Seguridad: la **Oficina de Gestión de Seguridad**. Se trata de una estructura de gestión que se responsabiliza de organizar y supervisar la colección de proyectos y líneas de acción definidas en el Plan Director. Se puede abordar su creación de forma interna a la organización o **externalizarla**, pero en todos los casos y dado su foco, deberá tener una componente importante en gestión de proyectos (un punto útil de partida puede ser el modelo de Oficina de Gestión de Proyectos propuesto por el PMI, *Project Management Institute*).

En ambos casos, es importante que dicha oficina no pierda el "foco" sobre su papel, y afronte sus decisiones desde una **visión global** de los objetivos de seguridad de la entidad. Otra de sus principales funciones es la de desarrollar estudios de situación y análisis de valor de organización, que puedan ser utilizados para justificar la inversión en seguridad de la información.

Ilustración 10.- Herramientas de Gestión del Plan de Seguridad.

El último aspecto que se debe recalcar sobre la Gestión de los Planes Directores de Seguridad es precisamente el relacionado con su control y supervisión. Como se expone a continuación, se pueden utilizar diversas aproximaciones para gestionar la operativa del Plan Director de Seguridad.

Para entornos sencillos o medianamente complejos es aceptable el uso de herramientas manuales, como por ejemplo las hojas de cálculo. Mediante una hoja de cálculo es factible representar cada una de las acciones definidas en el Plan Director de Seguridad e incluir los aspectos básicos que las definen (fechas, recursos y coste y responsable)

Sin embargo, en entornos más complejos (la complejidad no necesariamente implica una organización de mayor tamaño), se debe apostar por el uso de una herramienta específica que soporte la gestión del plan. Dichas herramientas aportan ciertas funcionalidades adicionales, en particular, a la hora de analizar la relación coste/beneficio de las acciones y en el seguimiento de las mismas. En todos los casos, el uso de una herramienta de gestión de riesgos es imprescindible, o al menos altamente recomendable. Su papel es servir como base para el análisis de riesgos y valoración de contramedidas, así como su posterior seguimiento, verdadera clave para mantener una gestión de seguridad viva.

Dejando el plano de gestión del propio Plan Director, es necesario también entender el papel que desempeña éste en el marco de la Gestión Estratégica de Seguridad. Existen diferentes concepciones sobre cómo se debe posicionar en relación con el resto de planteamientos dentro de la organización, que condicionan la mejor aproximación para plantear su creación:

- El enfoque clásico ubica al Plan Director de Seguridad como la iniciativa de más alto nivel dentro de la organización, que subordina al resto de planteamientos y sirve como sistema de control. En este escenario, la implantación de un SGSI es un proyecto más derivado del plan.

- En los últimos tiempos, y consecuencia del advenimiento y creciente importancia de los SGSI, el Plan Director de Seguridad ha sido parcialmente “desmitificado”. Según este enfoque, el Plan Director es una derivada de la implantación de un SGSI y sirve como herramienta de gestión en la implantación de los controles de seguridad propuestos.

Aunque ambas visiones son perfectamente válidas, y realmente se puede escoger cualquiera de ellas sin riesgo a utilizar un enfoque incorrecto, este libro adoptará la de Plan de Seguridad como herramienta de gestión derivada de la implantación de un SGSI. La motivación por la que se adopta este planteamiento es la ventaja de estandarizar los criterios de implantación de controles, más acorde a la filosofía de los SGSI.

Aunque está fuera del ámbito de este capítulo, y será tratado de forma más exhaustiva más adelante, es importante hacer ciertas aclaraciones: el Plan Director de Seguridad, según el planteamiento escogido, es la herramienta de gestión de controles de seguridad definidos en la norma ISO 27002. Esta norma identifica un conjunto mínimo de controles a considerar en la protección de los activos de la organización. Para cada riesgo identificado, se valora la aplicabilidad de los controles recogidos en la norma, y se recoge en un documento denominado "Declaración de Aplicabilidad".

En resumen, tanto si se decide escoger un enfoque tradicional como uno integrado en el SGSI, el Plan Director de Seguridad es la herramienta estratégica que permitirá justificar y comprender las acciones de seguridad que se deben abordar, alineándolas con el negocio de la organización.

◆ 2.4. La seguridad en las TIC: requisitos básicos

La seguridad en las TIC se define como la capacidad de las infraestructuras o sistemas de información de minimizar o prevenir, con un determinado nivel de confianza, ante accidentes o acciones malintencionadas que pueden comprometer la disponibilidad, autenticidad, integridad y confidencialidad de la información transmitida o almacenada y de los servicios que ofrecen las infraestructuras o sistemas para acceder a está información.

Actualmente las necesidades de seguridad en las organizaciones están basadas en tres componentes fundamentales para su implementación:

- **Las personas**
  - Profesionales de las TIC con formación especializada y acreditada.
  - Usuarios con niveles de educación para un uso responsable de las TIC.

- **La gestión.**
  - Los sistemas de Gestión de la Seguridad de la Información (certificables).
  - La seguridad englobada dentro de los procedimientos y procesos de negocio o actividad en las organizaciones.

- **Las tecnologías y sistemas de información y comunicaciones.**
  - Sistemas que cumplen certificaciones de calidad de la seguridad de los productos TIC.

Estos tres componentes y su interrelación son las base fundamental para implementar la seguridad en las organizaciones, provocando un mayor riesgo en la seguridad si alguno de estos componentes no es tenido en cuenta como parte de la seguridad TIC.

El objetivo principal de los responsables de Seguridad de la Información es saber en tiempo real qué está pasando en los sistemas que pueda ser relevante para la seguridad de la información de sus organizaciones y, en consecuencia, poder tomar decisiones que prevengan o minimicen las amenazas que pueden afectar a la organización.

La seguridad lógica y las tecnologías de protección han de implementar las medidas y controles que permitan prevenir y gestionar el riesgo de amenazas y han de ayudar a crear procesos automatizados tendentes a disponer de información sobre eventos completa, útil y de calidad en el momento que sea requerido y que, además, permitan la implantación de mecanismos para la extracción, preservación y conservación de evidencias y registros de utilización de las infraestructuras.

2.4.1. La seguridad lógica

La seguridad lógica implementa las tecnologías de protección mediante medidas y controles que permitan prevenir y minimizar las posibles amenazas a las que están expuestas las organizaciones. Esta seguridad lógica debe estar basada en el concepto de la defensa en profundidad.

El concepto de defensa en profundidad tiene sus orígenes en el siglo XVII (Vauban) y se basaba en los siguientes puntos:

- Los bienes que se protegen están rodeados de varias líneas de defensa.

- Cada línea de defensa participa en la defensa global.

- Cada línea de defensa desempeña un papel: debilitar el ataque, entorpecerlo, retardarlo o pararlo.

- Cada línea de defensa es autónoma (está prevista la pérdida de la línea anterior para evitar la pérdida del resto de líneas de defensa): la pérdida de una línea de defensa debilita a la siguiente pero ésta dispone de sus propios medios de defensa frente a los distintos ataques (cada posible proceso de ataque ocasiona su correspondiente defensa).

- Se ponen en marcha todos los medios para reforzar la defensa de las distintas líneas:

  - Adaptar la fortificación.
  - Muros para limitar los efectos de penetraciones.
  - Informarse de la situación en cada línea.

Este concepto de defensa en profundidad se utiliza actualmente en los ámbitos militares, industriales (industria nuclear) y de la seguridad de los sistemas de información, ámbito en el que nos centraremos.

Actualmente, el concepto de defensa en profundidad se ha adaptado al ámbito de la seguridad de los sistemas de información. Este concepto ha incluido nuevos principios que han tomado mayor relevancia en el concepto de la seguridad TIC:

- La información ha pasado a convertirse en la primera línea de defensa: la información debe alcanzar desde el registro de las amenazas efectivas, ataques comprobados e identificados, la detección de actuaciones sospechosas (indicios o precursoras de posibles ataques) hasta los comportamientos “anormales” dentro de la organización.

- La defensa se ha convertido en un concepto dinámico que permita adaptarse a los requerimientos de seguridad de la organización.

- Existen varias líneas de defensa coordinadas y ordenadas según su capacidad y las necesidades que requiere la organización de forma proporcionada (coste del activo/coste salvaguarda).

- La pérdida de una línea de defensa debe debilitar el ataque (al menos indirectamente proporcionándonos un máximo de información sobre la amenaza, su naturaleza, sobre el posible comportamiento y las posibles etapas que seguirá), esta perdida no debe ocasionar la pérdida de otras líneas de defensa sino por el contrario reforzarlas o adquirir un mayor conocimiento de la amenaza.

- Las líneas de defensa deben incluir el registro de las amenazas (aunque se limite a la detección de anomalías y el registro de trazas en caso de ataques no identificables) en todos los ataques posibles, permitiendo adquirir un mayor nivel de conocimiento y análisis de la situación generada por la amenaza.

- La defensa no excluirá medidas de carácter ofensivo para mitigar los efectos del ataque.

Un ejemplo de la implementación de la defensa en profundidad es el caso de un puesto de trabajo protegido por un cortafuegos y un antivirus contra los accesos no autorizados, el antivirus constituye la segunda barrera frente al intento de acceso de un código malicioso por intrusión, pero se transforma en la primera barrera si el medio desde el que proviene la amenaza es el correo electrónico, puesto que el mensaje de correo electrónico es autorizado por el cortafuegos.

En este momento, la seguridad lógica en las TIC debe adaptarse al concepto de una línea de defensa formada por barreras que estén coordinadas y proporcionen información a los responsables y especialistas de la Gestión de la Seguridad de la organización para que puedan tomar decisiones.

Las barreras que componen la línea de defensa estarán relacionadas con los niveles de gravedad y la reacción correspondiente en caso de superarse estas barreras de forma planificada dentro de la organización.

La seguridad TIC es una defensa global y dinámica:

- El concepto global implica que se debe entender como una línea de seguridad y no un conjunto de medios de protección independientes, toda la línea de defensa debe disponer de dispositivos y de medios que permitan la detección, monitorización y notificación ante las posibles amenazas.

- El concepto dinámico implica que se debe adaptar a las necesidades de la seguridad, permitiendo la toma de acciones de neutralización con el menor coste y tiempo posibles, la posibilidad de gestionar el riesgo, la generación de informes, la planificación de las reacciones y el enriquecimiento permanente gracias a la experiencia adquirida.

La implementación de la seguridad lógica debe tener como finalidad:

- Reforzar la protección del sistema de información mediante un enfoque cualitativo de las barreras de seguridad que permita verificar la finalidad y la calidad del dispositivo o control que proporciona la seguridad.

- Proporcionar un medio de comunicación que permita a los responsables de la organización la toma de decisiones y a los usuarios tomar conciencia de la gravedad de los incidentes de seguridad.

La seguridad en las TIC según el concepto de la línea de defensa debe centrarse en la implementación y las tecnologías que la van a sustentar.

La implementación de la seguridad debe estar basada en políticas válidas y probadas. Los sistemas y los usuarios deben participar en la generación de informes sobre incidentes y estar informados sobre posibles amenazas que pueden afectar a la organización.

El sistema de información debe contar con políticas dinámicas de actualización de las herramientas que sustentan la línea de defensa dentro de la organización.

Toda implementación de herramientas dentro de la línea de seguridad deben tener como requerimientos su gestión, seguimiento y control. Permitiendo realizar un análisis de las trazas que proporcionen para permitir detectar posibles incidentes.

La política de mantenimiento debe estar contenida dentro de la seguridad en profundidad, diversificando los proveedores, verificando y comprobando los contratos para verificar que cumplen con los requerimientos definidos en la política de seguridad de la organización.

La defensa en profundidad se debe basar en líneas de defensa tecnológicas coordinadas e independientes. No debiendo existir un punto único en el que se apoye toda la seguridad de la organización. Esto implica que la seguridad no debe basarse en una tecnología o un producto de seguridad (aunque tenga una calidad certificada).

Todo producto de seguridad debe ser controlado, protegido y proporcionar un plan de reacción en caso de incidente.

Es necesario limitar la exposición de los elementos de seguridad a las amenazas mediante la creación de zonas protegidas por cortafuegos y monitorizadas por sistemas de detección de intrusos y limitar sistemáticamente los servicios ofrecidos a los estrictamente necesarios (línea base de securización de los sistemas).

La defensa en profundidad en las tecnologías debe llegar a los puestos de usuarios y a los accesos a la infraestructura de la organización mediante tecnologías de cortafuegos personales, antivirus actualizados y de diferente tipo a los utilizados en las pasarelas de correo electrónico, actualización de los sistemas operativos y políticas de control de acceso en los puntos de conexión a la infraestructura de la organización.

La formación de los usuarios debe sumarse a todas las tecnologías que apliquemos en las infraestructuras y los puestos clientes, esta formación debe hacer conscientes a los usuarios del riesgo que tienen las organizaciones aún aplicando tecnologías en la seguridad de la organización.

2.4.2. Componentes de la defensa en profundidad

Las organizaciones deben aplicar la defensa en profundidad en base a una serie de capas o niveles aplicando las tecnologías que mejor se adapten a los procesos del negocio y los activos que tienen que proteger.

Estas tecnologías deben estar coordinadas y proporcionar información a los responsables de la seguridad para permitirles tomar decisiones y conocer el estado de la seguridad dentro de la organización.

El siguiente esquema muestra un ejemplo de defensa en profundidad aplicando distintos niveles y las posibles tecnologías que proporcionarían seguridad dentro de cada uno de ellos.

Ilustración 11.- Defensa en profundidad.

A continuación se detallan los niveles que componen la Seguridad Lógica dentro de las organizaciones y las tecnologías más comunes utilizadas en cada uno de ellos:

2.4.3. Seguridad en el perímetro

Es el nivel donde se delimitan las fronteras de la organización con el exterior. Este nivel ha sufrido cambios en las infraestructuras actuales, siendo muy difícil delimitarlo por la introducción de nuevas tecnologías (móviles, accesos remotos por VPN y redes wifi) que han provocado el aumento de los accesos y una pérdida de control de los límites del perímetro en las organizaciones.

En este nivel se deben implementar tecnologías que permitan:

- Delimitar los accesos desde y hacia la organización.
- Controlar y filtrar los accesos de entrada y salida de la información.

- Proporcionar seguridad de los servicios ofrecidos.

- Registrar y controlar los accesos que se han producido en el perímetro de la organización.

Se deben considerar múltiples aspectos para diseñar una infraestructura perimetral segura, los factores claves a considerar deben ser:

- Implementar una estrategia de seguridad basado en la defensa en profundidad.

  - Esto significa basar la seguridad en más de una tecnología o producto.

  - Utilizar las capacidades de seguridad que ofrecen los elementos que componen el perímetro (enrutadores, cortafuegos, detectores de intrusos, etc…).

  - Mantener una política de actualización de todas las tecnologías.

- Implementar tecnología cortafuegos.

  - Segmentar el perímetro en zonas delimitadas y protegidas mediante la creación de zonas externas, zonas desmilitarizadas y zonas internas.

  - Utilizar la tecnología de traducción de direcciones (NAT) para ocultar el direccionamiento interno.

  - Implementar los servicios externos (web, cCorreo, etc.) en zonas desmilitarizadas securizadas y controladas. Implementando reglas de filtrado para estos servicios.

- Implementar tecnología Proxy en los servicios comunes.

  - La tecnología Proxy proporciona un nivel de seguridad adicional evitando la exposición directa de los equipos internos con las redes externas.

  - Los servicios recomendados para aplicar la tecnología proxy son la navegación web y los servicios de mensajería.

- Utilizar el principio del “menor privilegio” en la política de accesos de la organización.
  - Por defecto se debe denegar todo si no está explícitamente permitido.
  - Las reglas de filtrado se deben basar en la necesidad de acceder. Los usuarios deben tener acceso a los servicios que tienen aprobados, denegando el acceso al resto de servicios.
  - Se utilizarán tecnologías de filtrado (enrutadores, firewalls, VLAN) para implementar la política de acceso.
- Securizar y chequear cada componente después de su instalación, para asegurar que realiza la función para la que ha sido asignado.
  - Los componentes se deben instalar de forma securizada (deshabilitar servicios inseguros, securizar las comunicaciones, eliminar accesos por defecto, etc…), las instalaciones por defecto o malas configuraciones pueden producir agujeros de seguridad en la organización.
  - Chequear de forma periódica la configuración y las reglas de filtrado para detectar posibles errores de configuración en los componentes.
  - Realizar auditorías de forma periódica para detectar posibles problemas de seguridad en las infraestructuras.

Una vez descritos los principales puntos a tener en cuenta en la securización del perímetro pasamos a describir las principales tecnologías que se están implantando en las empresas para proporcionar una seguridad inteligente y gestionada que nos permita tener un mayor nivel de confiabilidad y control en la seguridad dentro de nuestra organización.

2.4.3.1. Tecnología cortafuegos

La tecnología fundamental en la defensa en profundidad son los cortafuegos. Esta tecnología nos va a permitir regular el tráfico de información en diferentes niveles y zonas, proporcionando una protección ante los ataques tanto internos como externos dependiendo de cómo despleguemos nuestra infraes-

tructura de cortafuegos, segmentar nuestra red para proporcionar un mayor control de los accesos y servicios que ofrecemos y proporcionar un mayor nivel de privacidad y confidencialidad de las comunicaciones, protegiendo los activos de las organizaciones.

Actualmente ha surgido una nueva tecnología en la seguridad perimetral, que integra en una única solución varias tecnologías de protección denominados UTM (*Unified Threat Management*), son dispositivos que permiten gestionar las amenazas de una forma unificada en un sólo dispositivo, proporcionando la Gestión de la Seguridad en el perímetro en único elemento que realiza las funciones de antivirus de pasarela, filtrado cortafuegos y detección de intrusos. Como se ha indicado en los puntos anteriores, la seguridad no debe basarse en un único dispositivo, siendo estos dispositivos un elemento más en la defensa en profundidad. Dada la criticidad de este tipo de dispositivos es necesario elegir fabricantes que cumplan con garantías de calidad y fiabilidad en este tipo de sistemas.

2.4.3.2. Centro de Respaldo

Un punto clave en las organizaciones es la disponibilidad de sus servicios y sistemas, la información es un activo que tiene un gran valor para la organización, requiriendo de una protección adecuada.

Esta protección debe incluir el asegurar la continuidad del negocio en caso de una catástrofe que impida el funcionamiento correcto de la organización y sus activos.

Los usuarios tienen cada día más acceso a más información (electrónica). Este acceso implica exponer a las organizaciones a una mayor variedad de amenazas y generan unas necesidades de disponibilidad y continuidad de los procesos de negocio, que requieren de una gestión y un control por parte de los responsables de la información.

Estos requerimientos suponen la necesidad de disponer de soluciones que proporcionen una salvaguarda de la información y permitan la continuidad del negocio en caso de catástrofe total en la organización.

La solución existente para resolver el problema de la continuidad y disponibilidad de la información en las organizaciones son los Centros de Respaldo. Estos centros son una inversión, que nos va a permitir disponer de una infraes-

tructura que soporte el negocio de nuestra organización en caso de una catástrofe en los centros principales, permitiendo ofrecer los servicios fundamentales de acceso a la información y la continuidad de los procesos de forma temporal o parcial durante el tiempo que estén indisponibles los servicios en los centros principales de nuestra organización.

Las posibilidades que nos están dando las tecnologías en el ámbito de la disponibilidad de la información, la distribución de la información y las comunicaciones entre diferentes localizaciones, han hecho de los centros de respaldo un punto a tener en cuenta en todas las organizaciones con unos requerimientos críticos de acceso y disponibilidad de la información, siendo una solución fundamental para la continuidad del negocio de las organizaciones.

2.4.3.3. Control de acceso a la red

Actualmente las organizaciones tienen desplegadas infraestructuras de defensa perimetral que protegen a las organizaciones de las amenazas externas. Este enfoque de seguridad basado en la defensa del perímetro está cambiando. Hoy en día las organizaciones deben basar la seguridad en una defensa en profundidad en todos los ámbitos de la organización. La seguridad ha de basarse en un control tanto externo como interno de los accesos a la información que poseemos.

El control de acceso a la red (NAC – *Network Access Control*) ha surgido como solución a los problemas de seguridad de nuestra red interna, la red interna ha dejado de ser un entorno confiable en la que la disponibilidad y el acceso son prioritarios respecto a la seguridad.

Esta tecnología se basa en saber “quién”, “cómo”, “cuándo”, “dónde” y “a qué” conecta, realizándose un control de acceso mediante la identidad del cliente que trata de acceder a la red y el estado de cumplimiento de la política de seguridad.

Las organizaciones presentan una serie de características en las redes internas que suponen un gran riesgo para su seguridad:

- Acceso estático a redes. Puntos de accesos LAN no securizados.

- Todos los dispositivos están permitidos.

- Dispositivos móviles accediendo a diferentes entornos y organizaciones.

- Falta de control de dispositivos que no cumplen las políticas de seguridad.

- Acceso de colaboradores externos a nuestra red.

Las soluciones de control de acceso a la red nos van a permitir controlar y validar los accesos que se producen dentro de las redes internas de nuestra organización, ofreciendo una serie de funcionalidades que nos van a permitir minimizar los riesgos y definir una política de acceso en nuestra red interna. Las principales funcionalidades que nos ofrecen son:

- Entorno seguro de acceso a redes de forma dinámica basado en políticas.

- Permite la integración con las infraestructuras existentes.

- Control del cliente que accede mediante verificación y remediación antes de obtener acceso a la red interna.

- Evaluación del cliente de forma continua. Dispositivos infectados o que no cumplen la política de seguridad son tratados de forma separada al resto.

- La verificación y remediación automática puede escalar y responder rápidamente ante incidentes a gran escala.

- Las políticas de acceso proporcionan mayor control de la organización reduciendo el riesgo y el número de amenazas que afectan a la seguridad LAN.

- Los sistemas de remediación automática tienen un impacto positivo en organizaciones con grandes despliegues, reduciendo la inversión en recursos (automatización).

2.4.3.4. Centralización y correlación de eventos de seguridad

Las tecnologías de centralización y correlación de eventos de seguridad son la base para conocer el estado en el ámbito de la seguridad en el que se encuentra nuestra organización.

Las tecnologías de centralización y correlación de eventos de seguridad (SIM - *Security Information Management*) nos van a proporcionar la información necesaria para conocer el estado de nuestros sistemas, las posibles amenazas que estamos sufriendo y el registro de las mismas, proporcionando un mayor nivel de conocimiento y análisis de las amenazas a las que estamos expuestos.

Las tecnologías de centralización y correlación de eventos de seguridad nos van a permitir analizar y gestionar todos los datos que recibimos de nuestros sistemas y de los elementos que forman parte de la línea de defensa en profundidad de nuestra organización, para transformarlos en inteligencia y conocimiento útiles para los responsables que gestionan la seguridad en nuestra organización.

Estos sistemas se han convertido en parte fundamental de la Gestión de la Seguridad en las organizaciones, siendo una tecnología necesaria para proporcionar una mayor inteligencia en el ámbito de la seguridad dentro de nuestra organización, permitiendo gestionar y valorar los riesgos de nuestros activos y definir reglas que permitan priorizar y filtrar el tratamiento de posibles amenazas que puedan suponer un riesgo grave en nuestra organización.

2.4.3.5. Accesos móviles

Las organizaciones han sufrido un cambio importante en el concepto de la defensa basada en el perímetro. Hoy en día la red interna ha ampliado sus fronteras.

Las nuevas tecnologías y la movilidad de los usuarios han hecho que la seguridad perimetral que teníamos claramente definida en nuestra organización haya desaparecido. Los accesos remotos forman parte de nuestra red interna y es necesario protegerlos.

Los entornos de movilidad se han ampliado y han provocado el aumento en las amenazas a las que están expuestas las organizaciones. Las organizaciones disponen de infraestructuras de acceso móviles como:

- Redes wireless.
- Accesos de dispositivos móviles que conectan en otros entornos no controlados (portátiles, PDAs, smartphones, etc.).

- Accesos remotos (redes privadas virtuales, accesos telefónicos remotos, accesos GPRS/UMTS).

- Etc.

Estas infraestructuras de acceso móvil, requieren de un control y una gestión con herramientas adecuadas que nos permitan minimizar el riesgo al que está expuesta nuestra organización.

Algunas de las soluciones tecnológicas que nos van permitir ofrecer unos niveles de seguridad aceptables en los accesos móviles son:

- Políticas de acceso (Control de acceso a redes).

- Cifrado de los canales de comunicación.

- Autenticación fuerte en los accesos.

- Protección de las elementos wireless.

El cifrado de los canales de comunicación se realizará mediante infraestructuras de redes privadas virtuales (VPN) ofreciendo el cifrado de las comunicaciones en los entornos no controlados por la organización y proporcionando una validación adicional de los dispositivos que conectan a nuestras infraestructuras.

La seguridad en las redes wireless es un punto crítico en nuestras infraestructuras. Es necesario disponer de infraestructuras configuradas de forma segura por integradores con un alto nivel de conocimiento en la tecnología y la seguridad de este tipo de infraestructuras, implantándo infraestructuras con tecnologías WPA y WPA2, cifrado de la información mediante VPN y autenticación fuerte (claves y certificados) que nos permitan minimizar el riesgo que suponen estas infraestructuras dentro de nuestra organización.

El despliegue de dispositivos móviles (PDA, smartphones, etc.) también son críticos en la seguridad de nuestras organizaciones, estos dispositivos son utilizados en entornos no controlados de nuestra organización y presentan un gran riesgo de pérdida o robo, es por ello que deben ser tratados con medidas

especiales en el ámbito de la seguridad para minimizar los riesgos que pueden suponer para la organización.

Los repositorios cifrados que se tratarán en el siguiente punto son una solución recomendada para estos tipos de dispositivos móviles o portátiles.

2.4.3.6. Cifrado de la información (dispositivos y repositorios)

El cifrado de la información se ha convertido en una necesidad dentro de las organizaciones, las posibilidades de acceso a la información y el aumento de tecnologías que nos permiten almacenar y disponer de esta información fuera del entorno controlado de nuestra organización, suponen un riesgo que es necesario controlar por los responsables de la seguridad en las empresas.

Las tecnologías de cifrado de la información nos van a permitir controlar los riesgos del acceso no autorizado a la información.

Las tecnologías de cifrado de la información abarcan desde el cifrado de los discos físicos de los equipos (tanto PCs de sobremesa, como portátiles, dispositivos móviles, etc.), el cifrado de los dispositivos de almacenamiento removibles (almacenamiento USB, tarjetas de memoria, discos externos) hasta el cifrado de los repositorios o carpetas donde almacenamos la información.

Este cifrado se realiza con claves mediante algoritmos fuertes de cifrado, estas claves de cifrado deben ser gestionadas y controladas en los entornos corporativos, dada la criticidad de la información que están cifrando y la necesidad de recuperar en caso de una contingencia grave.

Estas tecnologías nos van a permitir cumplir con los requerimientos legales que nos exigen hoy en día las normativas de tratamiento de la información como la LOPD. La información siempre viaja cifrada aún cambiando de medio de almacenamiento.

Existen tecnologías en el cifrado de dispositivos móviles que proporcionan un pre-arranque mediante un sistema operativo propio para proteger los sistemas previamente al inicio del propio sistema operativo que tiene el dispositivo, garantizando que la información almacenada en estos dispositivos no es accesible ante una pérdida o robo del dispositivo.

Estas tecnologías suelen trabajar de forma transparente al usuario y no implican una pérdida significativa de rendimiento en los sistemas.

2.4.3.7. Sistemas de acceso documental

La información se ha convertido en uno de los activos más importantes para las organizaciones, la gestión y el control del acceso a la información debe formar parte de los procesos de seguridad de la organización. Hoy en día los sistemas que se encargan de realizar estas funciones son los sistemas de gestión documental.

Los sistemas de gestión documental han evolucionado desde los primeros sistemas de gestión de archivos por carpetas con control de acceso, a entornos más complejos que nos permiten relacionar los documentos entre sí y proporcionar una gestión documental basada en la semántica.

Esta tecnología permite la relación de la información y proporciona un entorno colaborativo que permite explotar todo el potencial y nos puede dar una correcta gestión de los activos de información que poseen las organizaciones.

Estos entornos se han convertido en una pieza fundamental en los procesos de negocio de muchas compañías, estando enfocadas a un concepto más operacional y de procesos organizativos como pueden ser sistemas CRM, ERP, gestión documental, etc.

La implantación de esta tecnologías no es algo trivial y deben ser protegidas de forma adecuada al gestionar uno de los activos más importantes de las compañías, la información.

2.4.3.8. Gestión de la identidad

El control de acceso a la información y a las infraestructuras de información no es una tarea fácil en las organizaciones. Los entornos cada vez más heterogéneos, el amplio abanico de aplicaciones disponibles en el mercado, el traspaso de las fronteras de la propia organización con infraestructuras desplegadas en clientes, partners y proveedores. Hacen de la gestión de identidad una pieza clave que han de tener en cuenta los responsables de seguridad en las organizaciones.

Las tecnologías de gestión de la identidad nos van a proporcionar un conjunto de procesos que permiten la integración dentro de los entornos TI del control de acceso de los usuarios de una forma centralizada, facilitando las tareas de gestión de usuarios en las organizaciones.

La gestión de identidad nos proporcionará los mecanismos necesarios para identificar, validar y autorizar a los usuarios que accedan a los sistemas TI. Los procesos que nos proporcionará la gestión de identidad serán:

- Autenticación (validación de la identidad de los usuarios) mediante mecanismos como contraseña, certificados digitales, *tokens* de acceso, tarjetas inteligentes, dispositivos biométricos, etc.

- Autorización o privilegios que tiene el usuario. A través de la identificación pueden conocer los privilegios y perfiles del usuario que acceda a los sistemas y a las aplicaciones que ofrece la organización.

Toda la gestión de estos procesos descansará en los servicios de directorios (generalmente LDAP) que actuarán como repositorios centralizados en los que se consolidarán y recopilarán los datos de acceso a los sistemas y a las aplicaciones que posee la organización.

Esta tecnología dispondrá de procesos para integrar mediante conectores los distintos sistemas y aplicaciones que poseen las organizaciones.

Como resumen de todo lo anteriormente tratado hay que tener en cuenta que la información es uno de los activos más preciados dentro de las organizaciones y es necesario protegerlo de forma adecuada, siendo esta protección realizada por un mecanismo que integre una línea de defensa coordinada y gestionada.

◆ 2.5. Gestión de la continuidad y recuperación de desastres

En los últimos años, la cantidad de servicios telemáticos ha incrementado considerablemente y los tiempos de respuesta deseados se han reducido a mínimos insospechados. Concretamente, aspectos como los acuerdos de nivel de servicio están a la orden del día y toman mayor relevancia paralelamente a la criticidad de los servicios ofrecidos. En consecuencia, la gestión

de la continuidad se ha convertido en uno de los grandes retos para la práctica totalidad de las entidades con un grado suficiente de dependencia tecnológica.

En algunos casos los servicios y procesos utilizados con anterioridad a la sistematización han sido sustituidos, en otros han sido completamente olvidados en detrimento de los servicios informatizados. Esta sustitución o erradicación ha permitido a las entidades disminuir costes y ocasionalmente elaborar modelos de negocio alternativos que han resultado de la generación de nuevas empresas y/o negocios. Sin embargo, también ha causado un impacto de consideración frente a la atención personalizada clásica, y ha marcado la dependencia del buen funcionamiento global de una entidad en una única oficina o sucursal basada en sistemas de información.

La automatización de servicios facilita la disminución de errores humanos ya que nada se tramita hasta que todos los requisitos se han cumplimentado satisfactoriamente. Por el contrario, esto ha supuesto una disminución considerable de esfuerzos en los trámites internos y en determinadas ocasiones la práctica erradicación de personal cualificado. Esta disminución de personal cualificado junto al olvido de los procesos antiguos hace que muchas entidades no se encuentren preparadas para trabajar manualmente en el momento en que hay una indisponibilidad de los sistemas, lo cual se ha convertido en un factor crítico a la hora de establecer estrategias de contingencia y continuidad.

En consecuencia, la automatización de servicios y procesos tiene sus ventajas e inconvenientes. Por un lado, pueden proporcionar una mayor eficiencia a las entidades y por otro lado puede incrementar sus riesgos operacionales.

Desafortunadamente, sólo nos acordamos de santa Bárbara cuando truena. Tienen que suceder eventos tan desafortunados como los del 11S o el incendio del edificio Windsor en Madrid para reflexionar sobre cuál sería el impacto que sufriría nuestra empresa si algo similar le sucediese a nuestros edificios. ¿Conseguiría nuestra empresa prevalecer? ¿Y sobrevivir? La condición humana hace que los responsables de las empresas sean reacios a pensar que algo de esas características les puede suceder.

Hoy día se puede pensar en diversos servicios como la tramitación de las declaraciones del IRPF, la facturación de los préstamos hipotecarios, la trami-

tación de los partes de siniestros de automóvil, el pago de las nóminas, etc.; sin embargo, es prácticamente imposible pensar en ellos sin los sistemas de información que los soportan. Curiosamente, hace no demasiados años, la mayoría de estas tareas se realizaban manualmente. A fecha de hoy esto resulta inimaginable.

Más aún, a día de hoy, no es necesario disponer del experto en recursos humanos que saca adelante las nóminas de la empresa; para ello, está el fabuloso ERP y el gabinete o la gestora subcontratada que resuelven todos estos problemas. Es tan simple como introducir los datos en los campos oportunos del sistema y mensualmente emite las nóminas sin mayor problema y con una precisión asombrosa.

El ejemplo del servicio de soporte de emisión de nóminas es particularmente bueno porque la práctica totalidad de la entidades lo consideran crítico y porque su disponibilidad impacta de forma muy distinta en las entidades según el sector en el que se encuentren, los actores involucrados, la estrategia de respaldo definida y la articulación de dicha estrategia.

De hecho, es completamente distinta la estrategia de respaldo a seguir en una entidad que mayoritariamente tiene oficinistas en nómina con un horario laboral regular que una entidad con un alto grado de temporalidad, turnos, pagos por horas y servicios como transportes. En el primer caso, la estrategia de respaldo puede ser tan sencilla como reenviar las nóminas del mes anterior a la sucursal bancaria, pues lo lógico es que los cambios sean menores. Sin embargo, en el segundo caso, definir esta estrategia de forma unilateral puede hacer que en caso de indisponibilidad de dicho servicio se paralice el negocio. De hecho en ocasiones, esto ha generado situaciones comprometidas como piquetes por parte de transportistas en más de una fábrica.

Por estas razones, es importante entender el negocio y analizar posibles escenarios antes de definir las estrategias de respaldo que dan soporte a la continuidad. Ante todo hay que involucrar a los actores apropiados y deben ser realistas.

Los planes de continuidad se pueden abordar de múltiples maneras; sin embargo, todas estas posibilidades tienen un denominador común que es la minuciosidad del resultado final. Un buen plan debe contemplar la recupera-

ción y los recursos necesarios para recuperar los servicios críticos en el tiempo determinado. Para ello, entre otras cosas, la entidad deberá:

- Ser capaz de detectar que un servicio crítico no funciona.
- Disponer de un equipo humano suficiente y preparado.
- Los recursos técnicos necesarios para la recuperación.
- Los procedimientos perfectamente definidos.
- Plan de ejecución probado.
- Mantener todo lo anterior actualizado.

Para ello, existen multitud de metodologías y estándares en el mercado. Entre ellos, se encuentra la BS 25999-1:2006 que propone abordar este tipo de proyecto mediante los siguientes pasos:

1. Entender el negocio.
2. Determinar la estrategia.
3. Desarrollar e implementar el plan.
4. Mantener el plan.

Esta propuesta es básicamente común a la práctica totalidad de las metodologías, que entre sí suelen variar poco; sin embargo, hay que saber qué partes son aplicables y cuál es el nivel de profundidad que se le quiere dar a las tareas que apliquen.

Por ejemplo, ¿es necesario realizar un BIA (*Business Impact Analysis*) detallado para determinar la criticidad de la totalidad de los servicios? Posiblemente, si se decidiese hacer un BIA detallado de la totalidad de los servicios en una primera iteración nunca se terminaría de desarrollar el plan de continuidad. En la mayoría de los casos es suficiente con determinar cualitativamente cual es el impacto de los servicios y realizar un BIA de determinados servicios sobre los cuales existen dudas.

De hecho, según el tamaño de la entidad, llevar a cabo un análisis de impacto en la totalidad del negocio de los servicios es en sí una tarea faraónica. Para determinados servicios está justificada. En otros una estimación cualitativa y supervisada es suficiente.

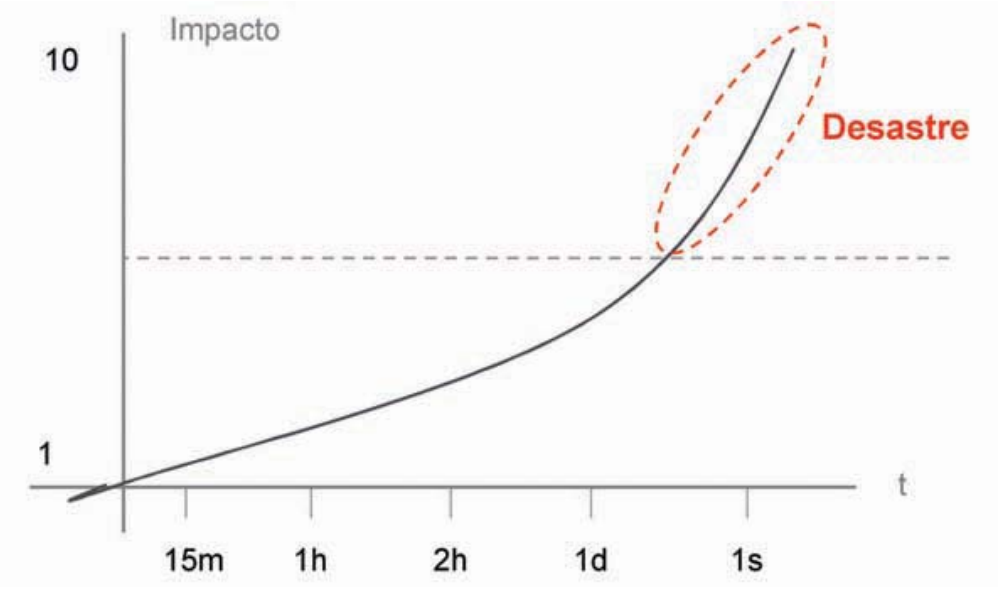

Ilustración 12.- El impacto determina cuándo un evento es desastre.

2.5.1. Entendimiento del negocio

Generalmente, se comienza analizando la estructura organizativa de una entidad. Obviamente, cuanto más cambie la organización más complejo será el posterior mantenimiento y actualización del plan y de la gestión de la continuidad.

Una vez identificada la estructura de la organización, se procede a la determinación de los distintos servicios primarios y de soporte de la entidad. Según el tipo de negocio, es importante diferenciar entre los destinatarios de los Servicios. En aquellos negocios en los que la imagen es un aspecto diferencial se suele considerar de mayor criticidad aquellos servicios que están directamente dirigidos al cliente final.

De este modo, a la hora de identificar los servicios se suele diferenciar entre los servicios primarios, aquellos directamente asociados al negocio de la entidad, y los de soporte que se corresponden con aquellos que ofrecen algún tipo de apoyo a los primarios.

A la hora de identificar los servicios es conveniente realizar una primera estimación del *Recovery Time Objective* RTO. Este es el tiempo que el responsa-

ble de servicio estima que la entidad puede operar sin dicho servicio sin causar pérdidas económicas de consideración.

Ser realista en la estimación de dicho indicador es un factor crítico, puesto que cuanto menor es este valor mayor será el coste de implementación de la estrategia de respaldo a seleccionar. Exagerando, si se decide que el RTO de todo es 0 horas, la única estrategia posible de respaldo equivale a la implantación de un sistema geográficamente redundante de la totalidad de los servicios primarios y de soporte. Es por ello, que el RTO estimado por el responsable de servicio, debe ser validado por una persona de mayor peso y con mayor conocimiento del impacto que la carencia de dicho servicio tiene sobre la entidad. Esto es fundamentalmente debido a que el éxito profesional del responsable de servicio está directamente ligado a la disponibilidad de dicho servicio, y para él siempre será crítico.

El siguiente paso incluye la priorización de los mismos mediante la ordenación de los servicios en base a su RTO. Si el trabajo anterior se ha realizado concienzudamente debería existir una gran variedad en el tiempo aceptable de disponibilidad. El siguiente paso es un factor crítico. Se trata de establecer una línea de corte que delimitará aquellos servicios para los cuales se establecerá una estrategia de respaldo y continuidad, y aquellos para los que no.

Huelga decir, que un servicio que hoy no se considera crítico pueda serlo mañana. Por ejemplo, los entornos de banca *on-line* no se consideraban críticos en sus inicios y a fecha de hoy se han convertido en una de sus mayores sucursales. En consecuencia, mantener actualizado el mapa de servicios y la selección de servicios críticos ayudará considerablemente a disminuir los costes de actualización del plan de continuidad en el momento que se decida oportuno; de otro modo, sería necesario repetir toda esta fase para la totalidad de servicios.

Para los servicios críticos de la entidad, se ha de proceder a determinar cuáles son los activos de la entidad que soportan dicho servicios. Entre los activos hay que pensar en dependencias físicas, en personal, en los sistemas y comunicaciones que dan soporte a los mismos, las aplicaciones, los datos, etc. Esta información es crítica para poder establecer las estrategias de continuidad oportunas.

Ilustración 13.- Ejemplo de RTO y RPO (datos necesarios para RPO).

2.5.2. Definición de la estrategia de respaldo y continuidad

Una vez determinados los servicios críticos, sus RTOs y los activos que soportan dichos servicios se propone la definición de la estrategia de respaldo. Para establecer dicha estrategia, es necesario definir genéricamente frente a qué escenarios se quiere estar preparado.

De este modo, no tiene porque ser la misma estrategia la que se defina frente al escenario en el que un edificio se incendie totalmente, que en el que se inunde el centro de proceso de datos, o simplemente haya una caída eléctrica prolongada.

Según los escenarios previstos, se contemplarán estrategias globales o parciales. Por ejemplo, si se contemplase un escenario equivalente al incendio de un edificio habría que establecer una estrategia global mediante la cual la entidad deberá respaldar la totalidad de los recursos asociados a los servicios críticos. De hecho, entre otros aspectos, deberá contemplar dónde ubicar a los empleados y con qué recursos.

Por otro lado, si se contempla una caída energética prolongada se definiría una estrategia parcial. Dicha estrategia podría estar basada en los grupos electrógenos existentes, en los sistemas de alimentación ininterrumpida y en el apagado eléctrico de todos aquellos recursos no considerados críticos, como por ejemplo los ascensores.

En consecuencia, es de especial relevancia y consideración saber contra qué se está preparado y contra qué no.

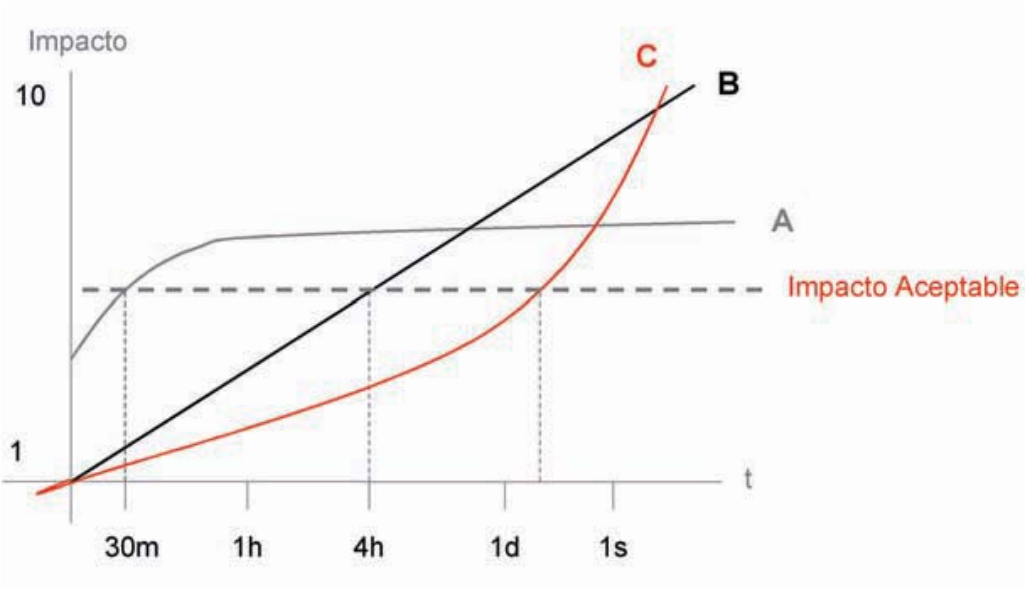

Ilustración 14.- Priorización de recuperación en base al impacto.

2.5.3. Desarrollo del plan de continuidad

El plan de continuidad tangibiliza lo mencionado con anterioridad. Establece los mecanismos oportunos para soportar las estrategias de respaldo y continuidad definidas.

Por un lado, se deberán establecer los mecanismos de monitorización tanto de los sistemas como de las dependencias críticas. Ser capaz de detectar un problema en su punto más temprano puede suponer una gran diferencia. De hecho, puede suponer la diferencia de tener que ejecutar el plan de respaldo o no.

Por otro lado, se deberán adquirir, alquilar, acordar y preparar todos los recursos necesarios para poder restaurar el servicio en el tiempo apropiado. De nada sirve preparar el mejor procedimiento de recuperación de un servicio o sistema crítico si a la hora de recuperarlo no existe un equipo donde instalarlo, no existen copias actualizadas de las aplicaciones y/o los datos.

Adicionalmente, el plan debe estar correctamente dimensionado, los recursos económicos, físicos, tecnológicos y humanos deben estar disponibles. Los recursos humanos deben estar asignados y formados para la ejecución

del plan de recuperación, y los procedimientos deben estar actualizados, publicitados, probados y no deben dejar pie a la improvisación.

2.5.4. Mantenimiento del plan

Disponer de un plan de continuidad desactualizado suele ser tan eficiente como no tenerlo. En consecuencia, después de haber realizado el esfuerzo considerable de elaborar el plan es una pena no haber asignado los recursos necesarios para mantenerlo actualizado.

Para ello, se pueden establecer mecanismos continuos y periódicos. Por ejemplo, se pueden asignar responsables y establecer procedimientos para mantener continuamente actualizada la matriz de los servicios críticos y sus RTOs, y actualizar el plan de continuidad anual o bienalmente.

Adicionalmente, es aconsejable establecer mecanismos continuos para actualizar el plan y los procedimientos en caso de que determinadas tecnologías o características como el almacenamiento hayan cambiado. En estos casos, es importante que los componentes del equipo de emergencia permanezcan formados acorde a dichas tecnologías.

◆ 2.6. Cumplimiento legal: LOPD, LSSI y otras regulaciones

En la actualidad hay dos leyes que marcan la diferencia en cuanto a su contenido, requisitos e impacto directo en el ámbito de los sistemas de información. Las dos leyes son la Ley Orgánica de Protección de Datos (LOPD) y la Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSICE). Adicionalmente, hay un proyecto de Ley que seguramente tendrá un mayor impacto sobre todo a corto plazo en los sistemas de información y en la seguridad de la Administración Pública. Es el Proyecto de Ley de Acceso Electrónico de los Ciudadanos a los Servicios Públicos, comúnmente conocida como LAE.

Las leyes en materia de protección de datos son de las primeras promulgadas que afectaban directamente a la seguridad de la información y fortalecen el Artículo 18 de la Constitución Española de 1978 en su apartado 4 que establece que “La Ley limitará el uso de la informática para garantizar el honor y

la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos."

Aquellos que desconocen la vigencia de las leyes en materia de protección de datos tienden a pensar que la legislación es reciente. Es necesario comprender, que este tipo de normativa existe desde la aprobación en 1992 de la Ley Orgánica para la Regulación del Tratamiento Automatizado de Datos (LORTAD), antecesora de la hoy vigente LOPD.

La LOPD "tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar." Y el ámbito de aplicación de la ley establece que "... será de aplicación a los datos de carácter personal registrados en soporte físico que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado."

Para ello, establece una serie de derechos a las personas físicas como es el derecho a la integridad de sus datos, de información, de accesibilidad, de intimidad, de rectificación, de cancelación y de indemnización. Es por ello, que la ley exige a las entidades que recopilan y manipulan datos de carácter personal que dispongan de los medios necesarios para articular dichos derechos.

La LOPD establece que las personas deben ser informadas de que sus datos están siendo recopilados, quién los está recopilando, la razón y el motivo por el cual son recogidos y mantenidos, para lo cual deben dar su aprobación. Adicionalmente, la entidad que obtiene y mantiene dichos datos debe articular los mecanismos necesarios para que el propietario pueda acceder a sus datos, modificarlos y/o cancelarlos.

Las entidades que recopilan y manipulan datos de carácter personal están obligadas a registrar los ficheros en la Agencia de Protección de Datos y a establecer una serie de requisitos organizativos, funcionales, documentales, procedimentales y técnicos. Estos requisitos se establecen en el reglamento de medidas de seguridad. El Real Decreto 994/1999, de 11 de junio, por el que se aprueba el reglamento de medidas de seguridad de los ficheros automatizados que contengan datos personales, establece que en función del tipo de datos personales manejados se deberán cumplir ciertas medidas de seguridad.

Para ello define tres niveles de seguridad exigidos según la naturaleza de los datos de carácter personal manipulados. Estos tres niveles son:

- **Bajo**: cualquier fichero con datos de carácter personal.

- **Medio**: datos relativos a la comisión de infracciones administrativas o penales, Hacienda Pública, servicios financieros, etc.

- **Alto**: los ficheros que contengan datos de ideología, religión, creencias, origen racial, salud o vida sexual así como los recabados para fines policiales sin consentimiento de las personas afectadas.

A modo de resumen, con el fin de poder mostrar el espíritu de los requisitos establecidos a continuación se muestra una tabla con algunos de los procedimientos básicos requeridos por el reglamento de medidas de seguridad según el nivel de seguridad.

	Nivel básico	Nivel medio	Nivel alto
Gestión de incidencias	Registrar la siguiente información: • tipo de incidencia • momento en el que se produce la incidencia • persona que realiza la notificación • a quién se le comunica • efectos que se hubiesen derivado de la misma	Indicar además: • procedimiento realizado de recuperación de datos • persona que ejecutó el proceso • datos restaurados • datos que han tenido que ser grabados manualmente Autorización escrita del responsable de fichero para ejecutar la recuperación de datos	
Control de acceso	Asignación, distribución y almacenamiento de contraseñas: • caducidad • almacenamiento ininteligible	Indicar además: • mecanismo de identificación de todo usuario que intenta acceder • límite en el nº de intentos de acceso	
Gestión de soporte	Inventario de soportes: • identificación clara del soporte • tipo de información que contiene • almacenamiento en lugar con acceso restringido	Sistema de registro de entrada y salida: • tipo de soporte • fecha y hora • emisor/ destinatario • nº de soportes • tipo de información que contienen • forma de envío • persona responsable de recepción/ salida	
Copias de respaldo y recuperación de datos	Garantizar reconstrucción de datos en caso de pérdida o destrucción semanalmente salvo que no haya habido actualización		
Pruebas de Sistemas de Información		Requerido	

Adicionalmente, contempla sanciones económicas de consideración en caso de incumplir los requisitos impuestos por dicha Ley o por el reglamento de medidas de seguridad. Estas sanciones se clasifican en tres según su gravedad:

- **Leve**: entre 601€ y 60.101€.
- **Grave**: entre 60.101€ y 300.506€ .
- **Muy Graves**: entre 300.506€ y 601.012€.

Por ejemplo, una infracción leve correspondería a no mantener continuamente actualizados los datos de carácter personal, una grave sería la creación de un fichero con fines distintos a los aprobados por el consentimiento del propietario y un ejemplo de incumplimiento muy grave, se correspondería a acciones como la cesión de datos sin consentimiento del titular.

El reglamento de medidas de seguridad, también establece que el responsable del fichero está obligado a la creación de un documento de seguridad actualizado con la descripción del fichero, funciones y obligaciones del personal, estructura del fichero, y otra serie de datos relativos al fichero.

Por otro lado, el objeto de la LSSICE es "la regulación del régimen jurídico de los servicios de la sociedad de la información y de la contratación por vía electrónica, en lo referente a las obligaciones de los prestadores de servicios incluidos los que actúan como intermediarios en la transmisión de contenidos por las redes de telecomunicaciones, las comunicaciones comerciales por vía electrónica, la información previa y posterior a la celebración de contratos electrónicos, las condiciones relativas a su validez y eficacia y el régimen sancionador aplicable a los prestadores de servicios de la sociedad de la información."

De este modo, la LSSI se aplica únicamente al comercio electrónico y a otros servicios de internet cuando sean parte de una actividad económica. Para ello, la ley exige que los sitios web muestren al usuario/cliente diversa información. Entre la información que deben publicar se encuentra:

- Denominación social, número de identificación fiscal, domicilio y dirección de correo electrónico.

- Códigos de conducta a los que se encuentren adheridos y donde poder consultarlos.

- Los precios de los productos o servicios que ofrecen incluyendo impuestos y gastos de envío.

- En el caso de que realizasen contratos *on-line*, deben informar sobre los trámites que deben seguir para la tramitación y las condiciones generales de dicho contrato.

- Confirmar electrónicamente la celebración del contrato mediante el envío de acuse de recibo del pedido realizado.

- Comunicar el nombre de dominio o dirección de Internet que utiliza el Registro Mercantil u otro Registro público en el que estuviesen inscritos.

Si también se ejerce una profesión regulada se deberán indicar:

- Los datos del colegio profesional y el número de colegiado.

- El título académico oficial o profesional y el estado de la Unión Europea en el que se expidió dicho título o la correspondiente homologación.

- Las normas profesionales aplicables al ejercicio de su profesión y los medios a través de los cuales se puedan conocer, incluidos los electrónicos.

La LSSICE establece otros artículos con requisitos específicos. Entre dichos artículos cabe destacar el artículo 18 que está enfocado a los operadores de redes y servicios de comunicaciones electrónicas, los proveedores de acceso a redes de telecomunicaciones y los prestadores de servicios de alojamiento que están obligados a recopilar y mantener los datos de conexión y tráfico generados por las comunicaciones establecidas durante la prestación de un servicio de la sociedad de la información por un período máximo de doce meses.

Por otro lado, la LAE es una ley que aún enfocada al ciudadano afecta en gran medida a la Administración Pública, su objeto establece que la "Ley reconoce el derecho de los ciudadanos a relacionarse con las Administraciones Públicas por medios electrónicos y regula los aspectos básicos de la utilización de las tecnologías de la información en la actividad administrativa, en las relaciones entre las Administraciones Públicas, así como en las relaciones de los ciudadanos con las mismas con la finalidad de garantizar sus derechos, un trata-

miento común ante ellas y la validez y eficacia de la actividad administrativa en condiciones de seguridad jurídica." Para ello "Las Administraciones Públicas utilizarán las tecnologías de la información de acuerdo con lo dispuesto en la presente Ley, asegurando la disponibilidad, el acceso, la integridad, la autenticidad, la confidencialidad y la conservación de los datos, informaciones y servicios que gestionen en el ejercicio de sus competencias."

Dicha ley afecta a la totalidad de la Administración Pública, a la Administración General del Estado, a las Comunidades Autónomas y a la Administración Local. Consecuentemente, dichas entidades se ven obligadas a modernizarse o a adaptar sus medios para poder facilitar el ejercicio de derechos y el cumplimiento de deberes por medios electrónicos. Para ello, las distintas entidades de la administración deberán:

1. Facilitar el acceso por medios electrónicos.
2. Crear las condiciones de confianza en el uso de los medios electrónicos.
3. Promover la proximidad con el ciudadano y la transparencia administrativa.
4. Contribuir a la mejora del funcionamiento interno de las Administraciones Públicas.
5. Simplificar los procedimientos administrativos.
6. Contribuir al desarrollo de la sociedad de la información.

Entre otros aspectos técnicos se consideran mecanismos como la autenticación para la cual deberán poner los medios oportunos conforme a la Ley 59/2003, de 19 de diciembre, de firma electrónica.

Adicionalmente, atañe directamente tanto a los servicios ofrecidos al ciudadano como a las relaciones entre distintos entes de la administración. En consecuencia, la administración se verá obligada a promover, establecer relaciones y poner en marcha los mecanismos oportunos para comunicarse tanto entre sí como con el ciudadano, ofreciendo la privacidad y seguridad oportuna para garantizar los derechos fundamentales.

◆ 2.7. Gestión de las auditorías, o cómo evaluar la realidad

La evaluación de la realidad es una tarea compleja pues cada persona y entidad tiende a tener percepciones propias. Obviando aspectos financieros como puede ser la adquisición de un entidad por parte de otra, los motivos

para la realización de las auditorías de seguridad son variados al igual que su tipología. De hecho, generalmente la motivación viene determinada por el grado de madurez o a raíz de situaciones indeseadas.

En determinadas ocasiones, se desea conocer el estado de la seguridad de algo específico como pueda ser el sitio web de la compañía, o la información que un empleado se ha podido llevar tras abandonar la entidad. Estas son situaciones que requieren un análisis específico y acotado.

En otras ocasiones se desea o se requiere verificar el estado parcial de la seguridad de la entidad, Este es el caso a la hora de determinar el grado de cumplimiento frente a la LOPD y el reglamento de medidas de seguridad, y esto requiere un análisis de mayor alcance, aunque, posiblemente no requiera el nivel de detalle del caso anterior.

Auditar algo pequeño o limitado es relativamente sencillo; sin embargo, cuando se trata de auditar la seguridad de una Entidad el tema se convierte en una tarea ardua y compleja. En estos casos, se requiere un análisis global estableciendo niveles de detalle en base a la relevancia de los activos de la entidad. Para ello es aconsejable disponer de una estructura normativa y documental. Si se desconoce la política, cuáles son las normas y cómo se espera que los empleados actúen y realicen sus tareas será difícil determinar la realidad de la entidad y si se están haciendo las cosas como se espera.

Mediante la política y el marco normativo se sabrá a grandes rasgos cuáles son los requisitos de seguridad de la entidad y en gran medida cuál es su marco de actuación y su grado de madurez. Adicionalmente, si existen resultados históricos o un Cuadro de Mando se podrán determinar dominios de seguridad en los que han ocurrido irregularidades.

Huelga decir que si existiesen recursos ilimitados, se podría auditar la totalidad con un grado de profundidad considerable. Sin embargo, este no suele ser el caso, por lo que es necesario determinar qué aspectos relevantes se han de auditar y hasta que nivel de detalle.

Por ejemplo, imaginemos que se decide auditar el grado de cumplimiento de la política de seguridad de las estaciones de trabajo de los empleados, obviamente, no es necesario auditar la totalidad de las estaciones de trabajo de la

entidad. Generalmente, se definirán distintas tipologías de usuarios y se seleccionará una población de ellos para extrapolar posteriormente los resultados.

Existe un continuo debate sobre si las auditorías las debe realizar personal de la propia entidad o se debe contratar a una empresa externa. Lo cierto, es que las auditorías debieran ser lo más objetivas posible. Generalmente, una empresa externa será "más objetiva"; sin embargo, no conocerá los recovecos de la entidad auditada. Con la finalidad de ser objetivos, es conveniente disponer de plantillas específicas para la realización de las auditorías. Considerando el ejemplo anterior, un auditor interno evitará entrar en conflicto con sus compañeros. En consecuencia, evitará ser exigente; sin embargo, si tiene que rellenar una plantilla en la que deba especificar concretamente los resultados de la misma, se estará responsabilizando de los resultados.

Por ejemplo, se pueden establecer las siguientes pruebas si la política de la entidad establece que el antivirus se actualizará continuamente, que queda prohibida la instalación de software que no sea corporativo y que no se podrán almacenar ficheros de uso privado.

- Nombre de la estación de trabajo.
- Dispone el equipo de antivirus (S/N).
- Antivirus (producto y versión).
- Fecha de la actualización del antivirus (–/–/–)
- Listado de las aplicaciones instaladas (Instrucciones para listar la totalidad de las aplicaciones instaladas en el equipo y guardarlo en un fichero – posteriormente se deberá verificar cuáles son y cuáles no son corporativas).
- Listado de ficheros (instrucciones para realizar búsquedas de ficheros mp3, jpg, etc.)

En otras ocasiones no es tan sencillo encontrar tal objetividad. Este es el caso por ejemplo de la auditorías técnicas intrusivas (test de intrusión, hacking ético, etc.). En esta tipología de auditorías hay que decidir entre buscar unos resultados homogéneos y su nivel de profundidad o detalle.

En este sentido, hay quienes prefieren o buscan un grado de seguridad medio para toda su organización y hay quienes prefieren buscar algo sencillo para la totalidad y algo profundo para sus aspectos más críticos.

Si lo deseado es un resultado homogéneo, la entidad puede basar la auditoría en la utilización de herramientas automatizadas o metodologías abiertas. En ambos casos, se sabe qué pruebas se están realizando y salvo cambios de versión, se obtendrán siempre los mismos tipos de resultados.

Por el contrario, en auditorías especializadas los resultados de la auditoría serán tan buenos como la experiencia y el conocimiento del auditor. De hecho, ocasionalmente identificar problemas es cuestión de experiencia e incluso intuición.

Otro aspecto de consideración, a la hora de planificar la auditorías es la periodicidad con la que se deben realizar. De hecho lo ideal es auditar con cierta frecuencia para verificar que el trabajo se está realizando correctamente. Sin embargo, es importante seleccionar y temporizar adecuadamente lo que se va a revisar. La periodicidad debería estar asociada a la capacidad y a los recursos disponibles para solucionar los problemas e incumplimiento detectados en la auditoría anterior. Salvo casos específicos, ¿para qué se querría analizar algo que sabemos que se encuentra exactamente en el mismo estado que la auditoría anterior?

En determinados casos, los aspectos a auditar y su frecuencia vienen determinados por elementos ajenos a una organización. Este caso, puede ser el que viene impuesto por la LOPD que determina que las auditorías se deberán realizar sobre un determinado tipo de ficheros y con una frecuencia bienal.

Otros de los aspectos que puede incrementar considerablemente la frecuencia en la realización de auditorías son los cambios. Estos cambios son muy comunes en determinados sectores en los cuales los cambios tecnológicos u organizativos están a la orden del día.

Finalmente, los resultados de las auditorías son otro factor importante. De poco sirve realizar un buen trabajo, en este sentido, si los resultados caen en saco roto. Una vez obtenidos los resultados de cualquier tipo de auditoría de seguridad se deberá realizar un plan de acción. Por un lado, se deberán priorizar las no conformidades y/o debilidades. Por otro lado, se deberá estimar el esfuerzo para solucionarlas. Se deberán asignar los responsables de solucionarlas, establecer fechas límite y canales de soporte y, sobre todo, articular los mecanismos apropiados para que no se reproduzcan.

En consecuencia, para gestionar las auditorías hay que tener claro cuál es el alcance, cuál es el nivel de detalle y profundidad que se requiere, analizar la posibilidad de homogeneizar las pruebas y los resultados, establecer una periodicidad sobre las pruebas a realizar, establecer los canales de comunicación para dar soporte en la corrección de las deficiencias encontradas, planificar la corrección de las deficiencias y en virtud de la gravedad verificar que han sido corregidas satisfactoriamente.

◆ 2.8. Cuadros de Mandos, métricas e indicadores: midiendo la seguridad

Antes de iniciar la descripción de lo que es y de lo que no es un Cuadro de Mandos de Seguridad, es necesario reflexionar primeramente sobre el origen de la necesidad que tiene una organización de disponer de herramientas de este tipo.

En la vida real, cualquier ser humano se enfrenta con la necesidad de saber en qué estado se encuentra su entorno, tanto en general como en aspectos particulares del mismo. Y para ello, se fija en el valor numérico de algunos parámetros que le son de utilidad para tener ese conocimiento. Así, consulta el valor de la temperatura del día para saber si hace frío o calor, mira su reloj para saber qué hora es, etc. Es decir, se establecen métricas e indicadores de la realidad.

Por la misma razón, en un entorno empresarial también se definen métricas e indicadores que ofrecen información sobre el estado de la empresa. No por el mero hecho de tener esta información disponible, sino para poder gestionar la empresa a través del conocimiento de su estado, pudiendo detectar situaciones no deseadas y pudiendo tomar decisiones adecuadas para evitar dichas situaciones. Es decir, para gestionar la empresa. Porque, como bien sabido es, sólo se puede gestionar lo que se puede medir. Con métricas e indicadores.

Partiendo de la necesidad de disponer de esta información, debe fijarse también la forma en que la información se transmite a sus receptores. Por ejemplo, pensemos en un automóvil, y en los indicadores que pueden existir en él. Posiblemente una métrica que vigile la mezcla de gasolina y aire en el carburador sea muy interesante desde el punto de vista de los mecánicos. Sin embargo, para el conductor no será muy relevante. Al conductor le pueden interesar más otros datos como la velocidad a la que circula, cuánta gasolina

le queda en el depósito o si hay algún sistema que está funcionando de forma anormal. El conductor necesita además saber cuándo el indicador le está transmitiendo una información particularmente importante, como ocurre cuando se aumentan las revoluciones del motor, y el cuentarrevoluciones entra en una zona marcada en color rojo. Ésta es la información que tiene el conductor a su disposición en el salpicadero del coche. En realidad, podría pensarse que el salpicadero tiene embebido el cuadro de mandos del coche, puesto que en él se recogen las métricas e indicadores que necesita el conductor (el gestor del vehículo) para conducirlo (realizar correctamente su trabajo de gestión).

Este último ejemplo sobre el cuadro de mandos de un coche puede dar la sensación de que al final un cuadro de mandos se resume grosso modo en una disposición más o menos acertada de un conjunto de números, relojes, colores y señalizadores que dan información en principio de utilidad sobre el estado del elemento que se está gestionando. En realidad, este elemento de visualización es importante, pero es solamente el final del proceso de captura de indicadores. ¿Qué es entonces un Cuadro de Mandos? ¿Qué falta en la visión descrita hasta ahora para un Cuadro de Mandos?

Siendo rigurosos, debe definirse un Cuadro de Mandos como una metodología o herramienta de gestión y operación de un sistema que refleja su situación actual, la planificación de acciones y el progreso realizado en la consecución de sus objetivos. Es decir, el Cuadro de Mandos incorpora en sí un conocimiento experto que permite:

- Identificar cuáles de todos los posibles indicadores de interés son realmente interesantes.

- Identificar cuándo estos indicadores quieren transmitir información de estado de especial relevancia, o que va a exigir una actividad concreta por parte del gestor.

- Asegurarse de que la información que transmite el indicador refleja fielmente la realidad

- Asegurarse de que la información es rápidamente transmitida y se facilita su entendimiento por el gestor que va a hacer uso de ella.

Además, en el caso de un Cuadro de Mandos de Seguridad (CMS) de una compañía, estos conceptos son aplicados y particularizados para las necesidades concretas de seguridad de la organización, la orientación y objetivos de seguridad que persigue y las medidas de control que la compañía tiene implantadas para mejorar su seguridad. Combinando todos estos puntos, el Cuadro de Mando de Seguridad es una metodología o herramienta de gestión y operación de seguridad que refleja la situación actual de la organización, la planificación de acciones y el progreso realizado en la consecución de sus objetivos. Para ello, el Cuadro de Mando refleja diferentes aspectos de seguridad, partiendo de datos automatizados o manuales tratados para su fácil interpretación según la definición de métricas e indicadores.

El Cuadro de Mandos es esencialmente una metodología de trabajo. Y esto se ve con claridad desde dos puntos de vista diferentes pero coincidentes. En primer lugar, en tanto que el Cuadro de Mandos de Seguridad recoge el estado de seguridad de la información de la compañía, puede utilizarse para que los distintos estamentos de la compañía conozcan dicho estado. Los estamentos de dirección de la compañía habitualmente estarán interesados en recibir reportes generales de estado de seguridad, mientras que el personal encargado de la operación y mantenimiento de los controles de seguridad de la compañía estarán más interesados en el estado de los controles que le son de su responsabilidad. Por lo tanto, el Cuadro de Mandos de Seguridad determina la forma en que el personal de la compañía debe realizar estas dos acciones y otras similares que sean necesarias.

En segundo lugar, el Cuadro de Mandos de Seguridad establece la metodología de conocimiento de la realidad de Seguridad de la compañía, y el resumen de la misma en un conjunto limitado de indicadores que permita su seguimiento. Habitualmente, una compañía tiene implantado un número elevado de controles de seguridad, cada uno de los cuales requiere ser gestionado mediante indicadores de seguridad. Además, existen otros elementos de la compañía que influyen decisivamente en la organización de seguridad y que deben ser incluidos en este esquema de trabajo, junto con sus indicadores correspondientes. El volumen de indicadores que se manejan habitualmente es del orden de los varios centenares y resulta excesivo. Por ello, el Cuadro de Mandos de Seguridad (CMS) debe incluir dentro de sí la capacidad de, sin perder contacto con la realidad, resumirla en un conjunto limitado de indicadores que sí puedan ser seguidos. Es decir, el Cuadro de Mandos consolida

los indicadores y métricas de seguridad de la organización. Esta actividad es vital, puesto que si se realiza de forma incorrecta producirá un Cuadro de Mandos no usable o que aporta información escasamente significativa.

Por otra parte, los indicadores deben estar bien calculados. Es decir, todos y cada uno de los indicadores han de tener claramente definidas las fuentes de información de las que se parte para su cálculo, la fiabilidad de las mismas, el proceso por el cual las fuentes producen el indicador y la frecuencia con la que se dispone de un nuevo valor para el indicador. Además, cada una de estas actividades respecto de un indicador debe ser correcta y eficiente, por cuanto que un fallo en la integridad en el procesamiento de un indicador impacta con total seguridad en el resto del CMS, produciendo una visión deformada de la realidad de la organización y pudiendo motivar la toma de decisiones erróneas.

El CMS incluye también las zonas de alarma en los indicadores seleccionados. Al igual que las zonas rojas del cuentarrevoluciones del coche, se trata de rangos de valores de los indicadores seleccionados que reflejan situaciones no aconsejables en la organización y habitualmente se definen en base a umbrales. Una vez que un indicador alcanza estos umbrales, el CMS emite alertas al personal oportuno para solicitar la atención del posible problema detectado y determinar el curso de acción adecuado ante esta variación detectada. Esta alerta detectada no tiene porqué corresponder con una acción puntual, que se detecta y se trata en tiempo real, sino que pueden existir diversos tipos de umbrales para diversos horizontes temporales. De esta forma, el CMS debe ser capaz de permitir detectar tendencias en la organización que, eventualmente, puedan derivar en situaciones no deseadas: incidentes, alertas, ineficiencias, etc. Por la misma razón, en un mismo CMS y sobre un mismo indicador se pueden establecer tantos umbrales como se estime necesario, modulando en cada uno de ellos la gravedad del problema y la prioridad con la que esta alarma ha de ser atendida.

En este contexto, es adecuado preguntarse si el CMS ha de ser el único Cuadro de Mandos que exista en la organización, supeditando cualesquiera otras herramientas similares a él, o si por el contrario, debe el CMS supeditarse a ellas. La respuesta no es inmediata, puesto que depende definitivamente de las herramientas concretas existentes, sus finalidades y operativas. En todo caso, parece deseable que el total de Cuadros de Mando de la compañía sean

consistentes unos con otros, de forma que la información que se muestra en cada uno de ellos no sea ni compartida ni contradictoria. Por ello, el desarrollo de un CMS debe realizarse de forma sincronizada con los elementos ya existentes en la organización. Siendo perfectamente aceptable que alguno de estos elementos se integre como parte del CMS (debería estudiarse cuidadosamente cómo ha de hacerse esta integración).

Ilustración 15.- Un ejemplo de construcción a varios niveles de un CMS.

Finalmente, el Cuadro de Mandos de Seguridad contiene como ya se ha mencionado anteriormente informaciones de diversos tipos y de diversas fuentes. Información que, por otra parte, no es uniformemente equivalente en lo que se refiere a la audiencia para la que dicho indicador se ha diseñado, ni los objetivos que persigue dicha audiencia. Algunos indicadores serán de interés para la dirección general, en especial aquellos que resumen y consolidan el estado de seguridad general de la compañía; por el contrario, el personal más operativo tendrá interés en los indicadores que afectan a sus responsabilidades habituales, o en los que se puede seguir la calidad del trabajo que ejecutan; los responsables de seguridad sin embargo estarán interesados en el conjunto completo de indicadores del CMS. Esta necesidad de desglose de los indicadores requiere que el Cuadro de Mandos se apoye en alguna herramienta tecnológica que permita implantar control de accesos por los usuarios a los indicadores. De esta forma, cada usuario debe disponer de visibilidad sobre la información que necesita para realizar su trabajo.

En definitiva, el Cuadro de Mandos de Seguridad de una organización es una herramienta metodológica de las organizaciones que permite integrar en un elemento único las actividades de seguimiento y/o reporte de la seguridad en la organización y de forma adaptada a la propia organización. A través de la consolidación de los diversos indicadores de seguridad identificados y el establecimiento de umbrales de tolerancia para los diversos indicadores seleccionados, pueden detectarse las alteraciones en el estado normal de la compañía, tendencias existentes, de forma que se pueda actuar. Por otra parte, el CMS puede integrarse en otros Cuadros de Mando integrales de que disponga la compañía colaborando para ofrecer una visión única del estado de la compañía. De esa forma, el CMS pasa a ser un elemento central en las actividades de seguimiento de la seguridad en las organizaciones.

◆ 2.9. Buenas prácticas de externalización de seguridad

La externalización (*outsourcing* en inglés) es sin duda una práctica con creciente popularidad en todos los ámbitos del tejido empresarial, pero que dentro del sector TIC está teniendo una incidencia especialmente alta. Los motivos de su éxito son múltiples, pero posiblemente los más relevantes son:

- Flexibilizar los costes de servicios tradicionalmente internos, que sobrecargaban la estructura de los departamentos de TI.

- Buscar ayuda de expertos reputados para cubrir áreas en las que no existe conocimiento suficiente en la organización.

- Disponer de servicios dimensionados en cada momento a las necesidades específicas del negocio de la Organización.

- Tener capacidad para que la Organización se focalice en su negocio, y pueda confiar ciertos procesos a un especialista. (“Zapatero, a tus zapatos” como recuerda el aforismo)

Una de las áreas donde mejor encaja este paradigma es precisamente en la de Seguridad de la Información. La externalización es habitualmente el modelo al que acuden organizaciones que tienen inquietudes en seguridad pero que, o bien carecen del personal apropiado, o no disponen de recursos o tiempo para poder acometer y focalizarse apropiadamente en dichas tareas.

La externalización es verdaderamente uno de los principales aliados de la Seguridad de la Información, pero su uso debe ser cautelosamente planteado y sus requisitos comprendidos y sopesados. A pesar de que la teoría dice que, cuando se externaliza, se debe preocupar del QUÉ y no del CÓMO, este planteamiento debe matizarse: los procesos que deben externalizarse son aquellos que aporten valor pero que permitan a la organización mantener el conocimiento de negocio de cada área. La externalización **feroz** en muchos casos ha finalizado con organizaciones con una dependencia total de un proveedor que ha pasado a conocer mejor el negocio que la propia entidad.

Asimismo, **externalizar** debe ser sinónimo de medir y supervisar: dado que se plantea el traslado de determinados procesos a manos ajenas a la entidad, su rendimiento y calidad en la ejecución deben ser controlados con especial atención. En auxilio de las organizaciones que decidan abordar la externalización parcial o total de sus servicios TIC, surgen diversas buenas prácticas de Gestión de Servicios. Sin duda el principal exponente es ITIL, corazón de la norma ISO 20000 y a la que se dedicará un breve capítulo más adelante.

Las buenas prácticas de Gestión de Servicios establecen diversos mecanismos que facilitarán de forma importante el control de servicios externalizados, siendo el más relevante para este caso el del SLA (*Service Level Agreement*, o Acuerdo de Nivel de Servicios). Su objetivo es fijar, mediante un contrato o acuerdo, los valores mínimos y el objetivo de rendimiento de cada servicio y establecer penalizaciones por su incumplimiento. Estos SLA se convertirán en parte integral del contrato de prestación de servicios establecido con el tercero y permitirán a la organización supervisar que la prestación se realiza de acuerdo a los parámetros de calidad establecidos.

Aunque todo lo comentado previamente es válido para la externalización de diversos servicios TIC, los relacionados con la seguridad tienen ciertas peculiaridades que deben ser completamente comprendidas y contempladas antes de planificar su externalización. El primer punto, base de una externalización satisfactoria, fue identificado ya en la antigua Grecia con la inscripción que figuraba en la puerta del Oráculo de Delfos: **"Conócete a ti mismo"**. Es altamente desaconsejable sacar de la organización cualquier proceso que sea crítico para el negocio, al menos de forma completa y sin garantías. Para ello, la entidad previamente deberá comprender de forma completa cuáles son sus procesos críticos y hasta qué grado pueden ser externalizados.

Otro caso especialmente relevante y que habitualmente lleva a confusiones, es el relativo a las organizaciones que disponen de un SGSI certificado y que desean externalizar servicios incluidos en el alcance de dicho SGSI. El modelo también resulta perfectamente válido para organizaciones que, aunque no disponen de un SGSI, quieren controlar apropiadamente la seguridad de sus servicios:

¿Se confía por completo en el prestador de servicios o se le obliga y controla que disponga de todos los controles que debe?

En esta encrucijada la propia norma ofrece pistas sobre cómo gestionar la situación:

- La "frontera" de seguridad, que separará los servicios externalizados de los propios, y donde ser reflejarán todos los requisitos de seguridad a cumplir por el proveedor será el Contrato de prestación de servicios. Éste deberá recoger de forma clara y específica todos los controles que la empresa prestataria deberá cumplir. Por ejemplo, en el caso de que los servidores de la organización se encuentren alojados en un datacenter externo, la empresa que lo gestione deberá acordar los mismos controles que debiera cumplir la organización en el contrato que regule la prestación de servicios.

- El contrato también deberá incluir otro requisito: la capacidad de auditoría. A través de esta cláusula, la organización podrá, en caso de considerarlo necesario, verificar que los controles incluidos en el contrato están efectivamente implantados y funcionando.

- Por último, se deberá tener en cuenta también la formación y concienciación del proveedor. El prestador de servicios y sus técnicos deberán conocer y cumplir las políticas y normas de seguridad establecidas por la organización, por lo que se deberán suministrar como parte del contrato y verificar que dichos técnicos lo conocen y cumplen.

Fuera del ámbito de los SGSI, pero sin duda parte integral de las buenas prácticas de externalización, existen consideraciones adicionales que deben ser atendidas:

- **Cumplimiento legal**: El caso más conocido y universal es el que tiene que ver con la protección de datos. En este sentido, será necesario con-

templar qué modelo de relación se va a establecer entre la organización y el prestador de servicios:

- Si se van a ceder o comunicar datos personales, la situación será regulada por el artículo 11, caso con un tratamiento específico muy estricto.

- Si el prestador de servicios únicamente va a tener **acceso** a los datos de carácter personal, se deberán atender a los requisitos definidos en el artículo 12.

En todos los casos, es altamente aconsejable disponer de asesoramiento experto, idealmente formado por un equipo mixto legal y técnico, capaz de aconsejar a la organización desde un punto de vista global.

A pesar de lo anteriormente dicho, el cumplimiento en absoluto se circunscribe a la protección de datos, y abarca gran número de áreas. En consecuencia, se deberán identificar todas las regulaciones que afectan a la organización y que deben ser cumplidas, ya sean legales, sectoriales o específicas de la propia entidad.

- **Confidencialidad**: aunque este apartado se toca de forma parcial en las consideraciones legales anteriormente mencionadas, es altamente recomendable formalizar este particular de forma independiente. Es común el uso de **Acuerdos de Confidencialidad**, que recogen el compromiso de proteger la información recogida en el servicio, no divulgarla y llegado el caso de finalización del mismo, destruirla apropiadamente. En servicios especialmente críticos es recomendable además del acuerdo de confidencialidad de organización, que cada uno de las personas que va a prestar el servicio firme un acuerdo particular.

- **Seguridad y SLA**: para servicios relacionados directamente con la seguridad, o que tienen implicaciones fuertes en este campo, es recomendable definir apartados específicos de seguridad en el SLA que regula la prestación del servicio. Este SLA deberá recoger desde aspectos relacionados específicamente con la seguridad a otros más genéricos, como aquellos específicos con sus variables, como la disponibilidad (por ejemplo, exigir que los sistemas de protección sean altamente disponibles).

- **Certificaciones de Seguridad**: como último punto, de forma similar a como se hace con las normas de calidad, es recomendable exigir a las compañías prestatarias de servicios externalizados que aporten certificaciones específicas de seguridad (como ISO 27001, UNE 71502 o incluso BS7799). Aunque la certificación del SGSI de la compañía que presta los servicios externalizados no es realmente garantía de que sus entornos sean seguros, sí lo es de que sus procesos de Gestión de Seguridad son apropiados y han sido auditados y certificados. Adicionalmente, y para la utilización de servicios específicos relacionados con otras prácticas (auditoría, Gestión de Seguridad, etc.), es muy recomendable exigir que el personal que los preste esté formado y disponga de las certificaciones más prestigiosas del sector (CISA, CISSP, CISM, GIAC, ITIL… la lista es larga y crece día a día.)

En cualquier caso, todos los procesos de externalización que se adopten en la organización deberán adaptarse a su cultura y necesidades específicas.

3. Marcos de referencia para la Gestión Estratégica de la Seguridad

La seguridad de los activos de información es un aspecto crítico para la organización. La dependencia de los servicios y procesos de negocio en la información y los medios para su procesamiento conlleva la necesidad de definir una estrategia de seguridad que garantice la salvaguarda de los mismos.

El gran reto es conseguir definir dicha estrategia y, lo que es más, desplegarla de forma que se consigan los objetivos de seguridad. A tal fin, a lo largo de los últimos años se han definido distintos marcos de referencia para la Gestión Estratégica de la Seguridad.

Estos marcos de referencia definen un modelo conceptual que ayuda a la organización a estructurar la función de seguridad. Como se verá posteriormente, estos modelos se apoyan fundamentalmente en el concepto de sistemas de gestión, con una clara orientación a los procesos.

Un elemento clave reconocido en todos los marcos de referencia es la necesaria implicación de la dirección. En efecto, el compromiso de la dirección transforma la seguridad de la información en un objetivo corporativo y garantiza la aportación de los recursos necesarios para darle cumplimiento.

Por otra parte, se refuerza el componente de gestión a través de la especificación de requisitos directamente vinculados con la identificación y captura de indicadores y métricas de seguridad. Como en todo proceso de gestión, la medición de los resultados obtenidos proporciona un camino de realimentación que permite a la organización determinar si los objetivos identificados han sido o no conseguidos.

Los marcos de gestión estratégica que se presentan comparten este conjunto de características, aunque difieren en su foco fundamental:

- ISO/IEC 27001 se centra en la implantación de un sistema de gestión para la seguridad, basado en el ciclo de mejora continua, al igual que otros modelos de gestión (calidad, medioambiental, etc.).

- COBIT 4.1 se centra en la definición de objetivos de control así como en el establecimiento de un modelo de madurez.

- ISO/IEC 2000 (ITIL) se centra en la definición de procesos de provisión y soporte de servicios IT, identificando de forma específica un proceso de seguridad.

◆ 3.1. Sistemas de Gestión de Seguridad (SGSI): ISO 27001 E ISO 17799

La madurez de las actividades de Gestión de Seguridad de la Información en las organizaciones dio un paso de gigante con la publicación en 2005 del estándar ISO 27001, primer y principal estándar de la familia 27000, orientada a este campo.

La familia 27000 consolida y estandariza a nivel internacional las diversas iniciativas nacionales que estaban en aplicación desde el final de la década de los noventa, como la serie BS:7799 en Reino Unido, o la norma UNE 71502 en España. Aunque la más popular de todas ellas era una norma ya internacional, ISO 17799. Esta norma se ha renumerado en 2007 en la Norma ISO 27002, dentro de la familia 27000. Todas estas iniciativas han sido aplicadas con éxito a nivel nacional en los últimos años en múltiples organizaciones. Así, a finales de 2006, existían cerca de 3000 organizaciones en el mundo que habían obtenido su certificación de seguridad, mediante la implantación y certificación de su Sistema de Gestión de Seguridad de la Información.

Porque esa es la propuesta principal de la familia ISO 27000: la implantación de un Sistema de Gestión de Seguridad de la Información. Como queda definido en el propio estándar, el sistema es la herramienta de que dispone la organización para llevar a cabo sus políticas y objetivos de seguridad. Dicho de otra forma, el sistema es la herramienta de la organización para dotarse en cada momento de las medidas de seguridad oportunas, que proporcionen los niveles de protección de la información que en cada momento sean necesarias, de la forma más eficiente, en un entorno de mejora continua.

Si analizamos la finalidad del Sistema de Gestión, deben destacarse algunos elementos claves de la misma, que definen perfectamente el valor de madurez que aporta un SGSI.

- Es una herramienta de la organización. Es decir, toda la organización debe participar en la aplicación de las medidas de control que se establecen, en la intensidad que le sea propia de acuerdo a cada una de las funciones definidas.

- Las necesidades de seguridad de la organización, y los niveles de protección necesaria asociados a dichas necesidades, pueden cambiar en el tiempo. Dicho cambio se reflejará en la modificación de los controles de seguridad que deben ser aplicados o la forma en que estos se aplican en la organización.

- La seguridad es un proceso de la organización. Afecta a toda ella y, como todo proceso, debe ejecutarse con la mayor eficacia posible.

- El Sistema de Gestión busca la mejora continua de seguridad. Es decir, no es suficiente con mantener los niveles de seguridad de que se dispone, hay que buscar las posibles mejoras en seguridad que se pueden conseguir, y aplicarlas.

El Sistema de Gestión tiene tres principales beneficiarios dentro de cualquier organización. El primer beneficiado es el propio responsable de seguridad de la organización. Sin el sistema, se ve obligado a recurrir a la intuición y experiencia para identificar las necesidades de seguridad y cómo atajarlas, respaldando con su prestigio estas decisiones. Si una decisión resulta errónea, su credibilidad queda afectada, así como su legitimidad para tomar futuras decisiones. El Sistema de Gestión cumple así una función de asistencia a la toma de decisiones, que respalda las del responsable de seguridad y facilita su comprensión al resto de la organización.

El segundo beneficiario es la dirección de la organización, y por ello ISO27001 exige su inequívoco respaldo al SGSI, tanto formal a través de la firma y apoyo a algunos documentos, como informal mediante el apoyo a la colaboración de otras áreas de la organización al sistema. La seguridad resulta en muchos casos un punto difícil, que la dirección sabe que hay que tener

pero que no sabe si se está realizando correctamente o las dinámicas que la afectan. A través del Sistema de Gestión, la dirección puede gestionar la seguridad en base a objetivos, recursos, planificaciones e indicadores, de forma semejante a como gestiona otras áreas de la empresa, sin tener que sumergirse en aspectos excesivamente técnicos. El Sistema de Gestión rompe la barrera de entendimiento que existía entre la dirección y el responsable de seguridad, origen de algunas leyendas urbanas populares como la del director general que pregunta en el ascensor al responsable de seguridad cómo estamos en seguridad, y otras semejantes.

El tercer beneficiario es la propia organización, que inicia una mejora sostenida en seguridad de la información. Dado que la seguridad evalúa todos los aspectos de seguridad, desde los más tecnológicos ligados a los Sistemas de Información hasta los de personal, seguridad jurídica, o la de instalaciones, todas las áreas de la organización van a poder mejorar y ser más seguras y eficientes en un momento u otro. Además, el personal de la organización va a ser consciente de la necesidad de seguridad en las actividades. La concienciación de seguridad (*security awareness*) ayuda así a la motivación de todos los miembros de la organización, puesto que todos ellos tienen un papel claro en la aportación de seguridad a la compañía.

Comenzaremos la descripción de la familia ISO 27000 con el estándar 27001, que formalmente se encarga de la definición de qué es un Sistema de Gestión de Seguridad de la Información y qué requisitos debe satisfacer, tanto desde el punto de vista de ciclo de vida y procesos ajenos al mismo, como de herramientas utilizadas, documentación y otros aspectos que deben integrarlo. Por lo tanto, al establecer un conjunto de requisitos para el sistema, estos pueden ser verificados por un tercero que emita un certificado de cumplimiento de los mismos. Por ello, es el estándar ISO 27001 el único que puede ser certificado.

ISO 27001 describe una metodología de trabajo, el ciclo de mejora continua en que se apoya la operativa del Sistema de Gestión de Seguridad de la Información. Se trata de un ciclo PDCA, que se recorre en cuatro fases: Planificación (letra P, *Plan* de PDCA), Implantación (letra D, *Do*), Verificación (letra C, *Check*) y Corrección (letra A, *Act*).

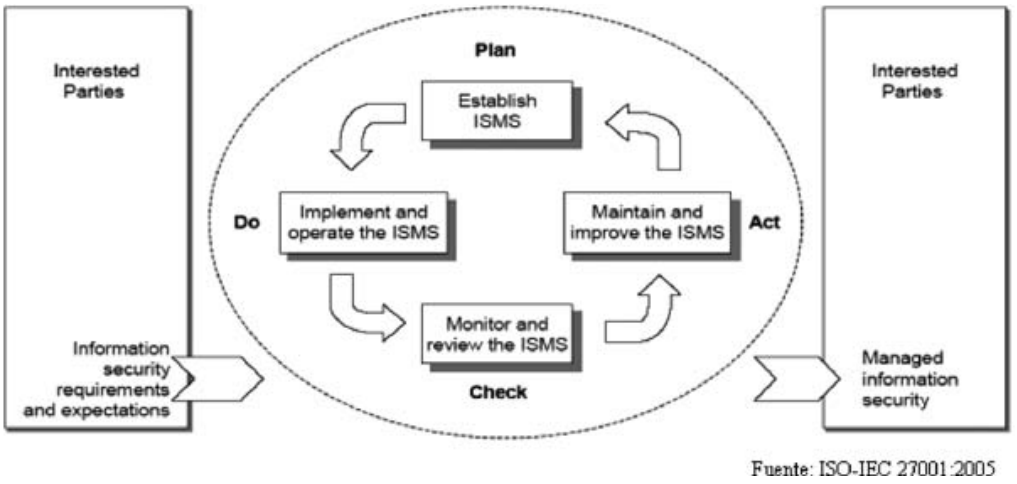

Ilustración 16.- Visión del ciclo de mejora de ISO 27001.

La fase de planificación asume las tareas de definición del Sistema de Gestión de Seguridad de la Información. Comienza por la definición de cuáles son los objetivos de seguridad que persigue la organización, y del ámbito en el que espera que dichos objetivos sean alcanzados. Los objetivos de seguridad quedan recogidos en la política de seguridad de la organización, mientras que el documento de alcance especifica el ámbito mencionado. Debe reseñarse en este punto que la decisión sobre el alcance del Sistema de Gestión es un punto definitorio del resto de la vida del sistema, por cuando condiciona decisivamente el volumen de actividades. Cualquier organización que implanta un SGSI aspirará al menos implícitamente a que el sistema le cubra por completo, aunque es viable cumplir esta aspiración mediante la implantación en un ámbito más reducido y su posterior ampliación dentro del proceso de mejora propio del sistema. Para ser exitosa, esta estrategia requiere de un conocimiento profundo de los Sistemas de Gestión y su implantación.

Una vez decididos los objetivos de seguridad y alcance de los mismos, el Sistema de Gestión inicia una fase de inventario, en la que se identifican e inventarían los activos de la organización incluido dentro del alcance. El inventariado es más que un simple conteo de servidores, o de bases de datos. Está orientado a la producción de resultados prácticos que mejoren la compañía, ya sea en su eficiencia, en los servicios y/o productos que ofrece, en el cumplimiento de sus objetivos y finalidades, o en sus resultados meramente

económicos. Por ello, es fundamental que el inventario se base en los procesos de negocio que desarrolla la organización, en las actividades que en ella se realizan, e incluir todos los recursos en que se apoya la organización para la ejecución de los procesos. Las tareas de inventario no se limitan simplemente a la recolección de información; se requiere que identifiquen y marquen los vínculos que existen entre los diversos activos identificados, y que condicionan cómo quedan protegida en cada activo la confidencialidad de la información que maneja el activo, su integridad o su disponibilidad.

A continuación, el Sistema de Gestión realiza un análisis de riesgos sobre los activos identificados en la fase de inventario. No se abundará aquí en la descripción de qué es un análisis de riesgos, diferencias entre análisis cualitativo y cuantitativo, o metodologías de análisis de riesgos existentes. Sí se debe tener en cuenta que el análisis de riesgos de un SGSI busca conocer cuál es estado de seguridad real de cada activo y el porqué de dicho estado: qué aspectos motivan que sea mejor o peor, qué activos "arrastran" por su mal estado de seguridad a otros, etc. Es decir, conocer la realidad actual de la organización en materia de seguridad de la información, para poder aportar su mejor valor, el valor de corrección de los problemas de seguridad que realmente existen. Y la detección y valoración sistemática de dichos problemas, de forma que se tenga que depender de la intuición del responsable de seguridad.

A la conclusión del análisis de riesgo, cada activo tiene identificado su nivel de seguridad. Su "nota" de seguridad. En este momento, el sistema está en condiciones de identificar los riesgos principales de la organización y sus activos en situación de mayor riesgo, y la forma de controlar estos puntos débiles. La respuesta a esta información se plasma en el documento de selección de controles, que identifica:

- Los riesgos que ya están siendo adecuadamente tratados y que no requieren de más actividades en este momento.

- Los riesgos que se van a tratar y la forma en que se va a realizar dicho tratamiento, detallando las medidas concretas que se implantarán, cómo se va a medir su efectividad y los recursos que requieren para su implantación. Esta información constituye el plan de acción de la organización, para la mejora de seguridad.

- Los riesgos que, en este momento, no se van a tratar y que la organización conscientemente acepta. Estos riesgos incluyen riesgos de muy escasa peligrosidad (bien por afectar a activos poco relevantes, amenazas poco frecuentes, etc) o aquellos que siendo relevantes son menos prioritarios que otros más importantes y cuya atención agota el presupuesto disponible. En ese sentido, debe recordarse que el SGSI es un ciclo de mejora continua, que no requiere que la ejecución simultánea de todas las actividades para conseguir la máxima seguridad de forma inmediata, sino que se ejecuta en varias iteraciones. Por ello, habitualmente los riesgos que se tratan en la iteración enésima del ciclo son riesgos que ya habían sido identificados y asumidas en iteraciones anteriores. Esta aceptación se plasma en el documento de aceptación del nivel de riesgo residual.

- El nivel de riesgo para la organización resultante de estas actividades.

De esta forma se cierra la fase Plan del ciclo PDCA descrito en ISO 27001, pasando a la fase *Do*. Esta fase se encarga de la ejecución del plan diseñado, usando metodologías de gestión de proyecto, integrando las soluciones tecnológicas de seguridad adecuadas, etc.

La fase *Check* se encarga de la verificación en el día a día de los resultados que se obtienen en seguridad en la organización. Para ello, se apoya en dos herramientas fundamentales:

- Indicadores de seguridad, habitualmente recopilados en formato de Cuadro de Mandos. Estos indicadores vigilan en tiempo cuasi-real la eficacia y eficiencia de las medidas de control previamente seleccionadas, y su operatividad a lo largo del tiempo, detectando desviaciones que requieran atención adicional.

- Actividades de auditoría de seguridad, que monitorizan el cumplimiento de otros controles en períodos de tiempo más largos.

Finalmente, la fase *Act* se encarga de la ejecución de los ajustes necesarios para conservar el estado de seguridad y para eliminar los problemas menores que se van detectando en la operación y mantenimiento del sistema. Si bien la mayor parte de sus actividades se deriva de los hallazgos de la fase *Check*,

esta fase se encarga también de imprevistos, habitualmente llamados incidentes de seguridad, contingencias o más comúnmente aún, respuesta ante ataques. Dentro de estas actividades se enmarcan la disponibilidad de equipos de respuesta ante incidentes (CSIRT), análisis forense, etc. El estándar no requiere explícitamente estos elementos, pero sí exigen que la organización se dote de capacidad de respuesta ante estas circunstancias.

Estos son los contenidos de ISO 27001. Como se ha podido comprobar, un SGSI es una herramienta de cierta complejidad, que incluye actividades muy diversas y que requiere de conocimientos multidisciplinares. Es precisamente esta necesidad la que da origen al resto de los estándares de la familia.

El segundo estándar de la familia, y posiblemente el más popular, es ISO 27002. Su título "Guía de buenas prácticas para la implantación de la seguridad de la información" es perfectamente descriptivo. Se trata de una lista de ideas, de sugerencias, de posibles controles de seguridad, que nos ayudan a implantar la seguridad de la información. Es decir, en el proceso anterior del Sistema de Gestión, cuando hay que decidir qué debemos hacer para controlar los riesgos de seguridad identificados en el análisis de riesgos, se debe acudir a este estándar para encontrar el control de seguridad que permite resolver el problema de seguridad identificado. En realidad, si alguna organización decidiera implantar el total de controles descritos en ISO 27002, tendría un nivel de seguridad elevadísimo. Y posiblemente, el tiempo y recursos necesarios para conseguirlo serían claramente ineficientes. Por ello ISO 27001 identifica los problemas que hay y qué controles merecen la pena ser implantados (y con qué recursos), dejando la parte más tecnológica de cómo hacerlo a ISO 27002.

ISO 27002 contiene 133 controles de seguridad, ordenados en 39 objetivos de control y en 11 capítulos: controles relativos a la política de seguridad, organización para la seguridad, clasificación y control de activos, recursos humanos, seguridad física, seguridad en comunicaciones, control de acceso, desarrollo y mantenimiento de SS.II., gestión de incidentes de seguridad, continuidad de negocio y conformidad legal (también llamada *Compliance*). Dentro de estos capítulos encuentran acomodo para su tratamiento algunos aspectos tan comúnmente aceptados y en boga en estos momentos como la formación en seguridad (en recursos humanos), la externalización de servicios (en organización para la seguridad), la implantación de planes de conti-

nuidad de negocio y centros de respaldo (un capítulo completo dedicado a esta disciplina), LOPD (dentro de compliance), CERTs (un capítulo completo dedicado a la gestión de incidencias y otros. Por lo tanto, el Sistema de Gestión nos va a permitir englobar dentro de una misma iniciativa múltiples aspectos necesarios para las organizaciones que hasta ahora se podían estar gestionando de forma desagregada, y con un soporte común para la toma de decisiones y selección de las actividades que deben realizarse, orientado al negocio.

El siguiente estándar en popularidad es ISO 27004, orientado al soporte de métricas e indicadores de seguridad, que han sido requeridos en diversos momentos por el Sistema de Gestión. El estándar propone ejemplos de métricas de seguridad que pueden ser aplicables en un SGSI, pero mucho más importante, describe la forma en que dichas métricas e indicadores de seguridad deben ser seleccionados, evaluados e implantados en el marco de un SGSI.

Finalmente, hay algunos estándares adicionales, no publicados en la fecha de edición de este libro, como son ISO 27000, que dota de un glosario común al resto de estándares; ISO 27005, que propone una metodología estándar de análisis de riesgos; y otros. En fechas próximas, asistiremos a su publicación.
El total de actividades de implantación de un Sistema de Gestión proporciona ya a las organizaciones la capacidad de gestionar de forma eficiente su seguridad. La certificación de las mismas a través de un tercero proporciona además el refrendo acreditable de ese trabajo. Un sistema de gestión puede no estar certificado y ser perfectamente operativo. Su certificación sería ya el remate final, su reconocimiento, la guinda del pastel.

◆ 3.2. Gobierno Corporativo y seguridad: COBIT

COBIT® 4.1 (*Control Objectives for Information and Related Technology*) es el marco de gestión definido por ISACA (*Information Systems Audit and Control Association*), una organización de sin ánimo de lucro fundada en 1969 y que aglutina más de 65.000 profesionales de más de 140 países.

COBIT® define un marco de gestión orientado a facilitar la gestión de las tecnologías de la información mediante la especificación de un modelo de gobierno, gestión y control. COBIT® se centra fundamentalmente en conceptos de control y menos en aspectos operativos.

COBIT® parte de un concepto sencillo: la relevancia de la gestión de las tecnologías de la información y las comunicaciones en la consecución de los objetivos de negocio. Por lo tanto, el gobierno de la función TI se convierte en un aspecto crítico para organización.

El gobierno de la función TI es una responsabilidad corporativa que engloba el liderazgo, la estructura organizacional y los procesos que garantizan que la función IT soporta las estrategias y objetivos corporativos.

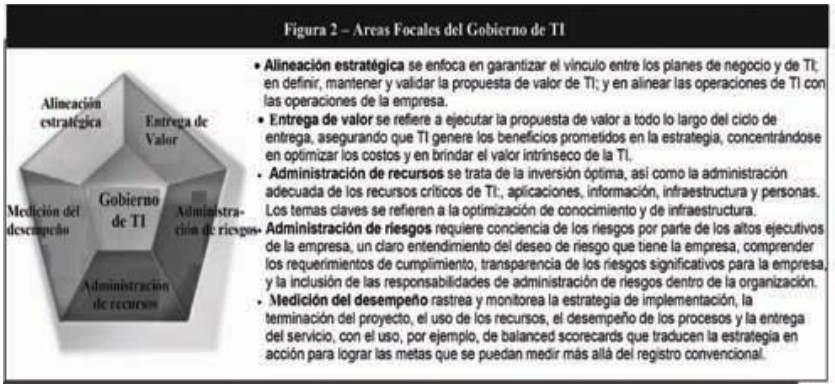

Ilustración 17.- Áreas focales del gobierno TI (Fte. ISACA).

Con el fin de garantizar que la función TI es capaz de satisfacer los requisitos de negocio, COBIT® propone desplegar un marco de control que permita:

- Vincular las necesidades negocio con la función TI.
- Organizar las actividades TI entorno a un modelo de procesos.
- Identificar los recursos TI necesarios para conseguir los objetivos.
- Definir objetivos de control para la función TI.

La orientación de negocio del modelo propuesto por COBIT® se basa en la vinculación de los objetivos de negocio con objetivos propios de la función TI, proporcionando métricas e indicadores que permitan medir su desempeño, estableciendo un modelo de madurez y definiendo un esquema de responsabilidades compartido entre las áreas de negocio y TI. El foco en procesos en COBIT® se traduce en la definición de un modelo de procesos que contempla 4 dominios y 34 procesos. La siguiente ilustración muestra la división en dominios y procesos sugerida por COBIT®.

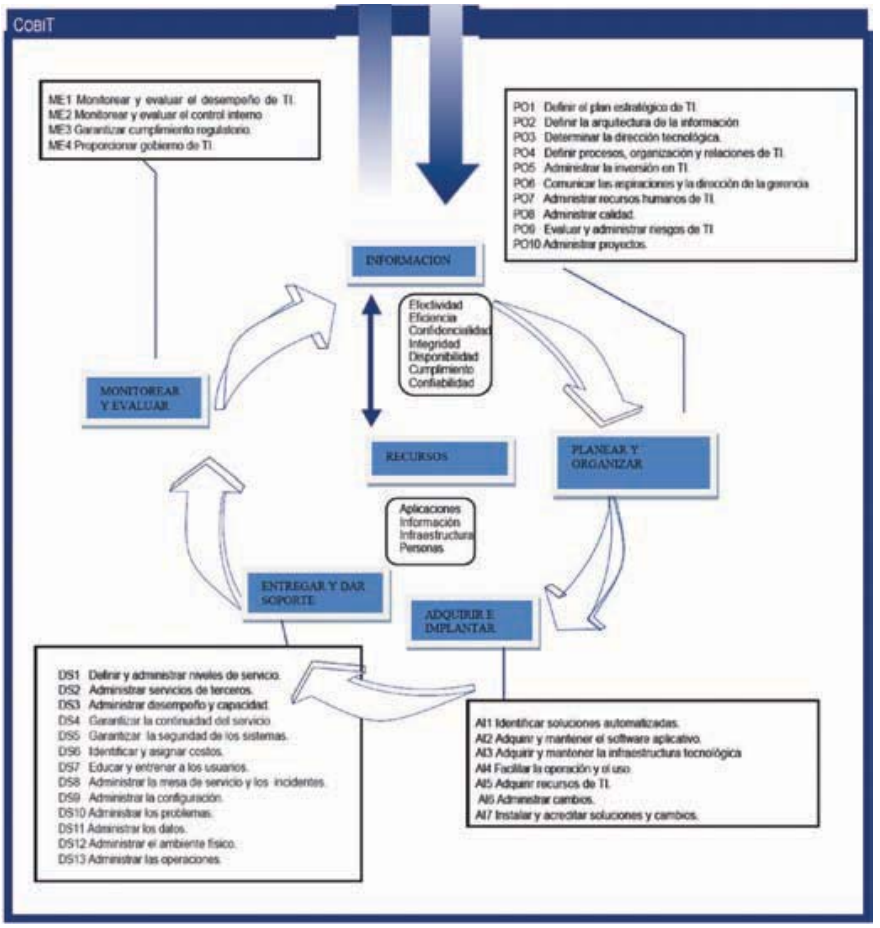

Ilustración 18.- Marco de trabajo COBIT® (Fte. ISACA).

COBIT® especifica objetivos de control para cada uno de los procesos definidos al tiempo que establece diversos mecanismos para evaluar la consecución de los mismos:

- *Benchmarking* de la capacidad de los procesos, expresada a través del modelo de madurez propuesto por COBIT®.

- Metas y métricas para los procesos TI con el fin de definir y medir su desempeño y resultados.

- Metas de actividad para el control de los procesos.

La relación entre los distintos componentes del modelo COBIT® se representa en la siguiente ilustración.

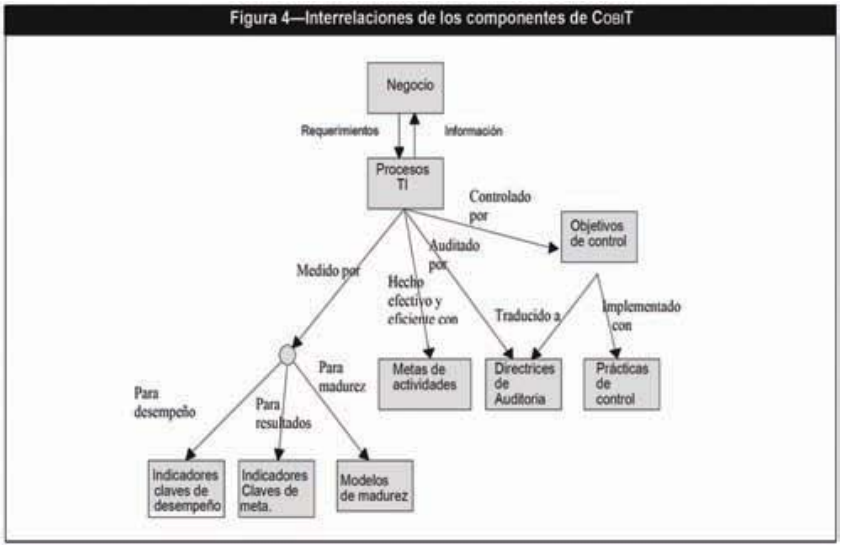

Ilustración 19.- Componentes del COBIT (Fte. ISACA)

◆ 3.3. Gestión de Servicios TI: ITIL/ISO 20000

El presente apartado trata de describir someramente la norma ISO/IEC 20000:2005 Tecnología de la Información – Gestión de Servicios, UNE ISO/IEC 20000:2007 en el esquema español publicado por AENOR. No se trata pues de describir exhaustivamente dicha norma, sino de destacar ciertos puntos clave de la misma sobre seguridad de la información.

La norma UNE ISO/IEC 20000:2007, nace de la adopción de la británica BS 15000 (revisión del 2002) como respuesta a la demanda de las organizaciones, y departamentos TIC de las mismas, de disponer de una norma que permitiera auditar y certificar un Sistema de Gestión de Servicios de Tecnologías de la Información.

Al igual que para el desarrollo de Sistemas de Seguridad de la Información se dispone de referenciales para requisitos, tales como ISO/IEC 27001:2005, y mejores prácticas. UNE ISO/IEC 17799:2002, esta norma se estructura en dos partes. La primera, UNE ISO/IEC 20000:2007-1, trata de las especificaciones del Sistema de Gestión de Servicios de Tecnologías de la Información y es la parte auditable de la norma, y, la segunda, UNE ISO/IEC 20000:2007-2, recopila una serie de buenas prácticas para dar respuesta a cómo cumplir las especificaciones de la parte 1 de la norma. La norma en sí no implica el uso de ITIL ni su adopción, sin embargo dado su origen histórico, su parte 2 recoge, en buena lógica, los procesos que predica ITIL.

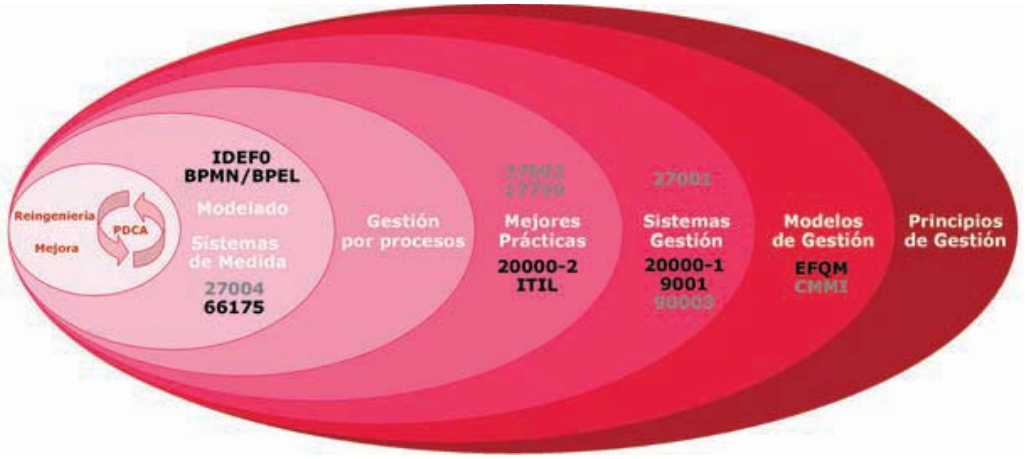

Ilustración 20.- Marco Conceptual y algunas referencias a modo ilustrativo.

La filosofía y la aproximación que debe realizar cualquier organización, que adopte esta u otra norma, en el desarrollo de un Sistema de Gestión propio, en este caso de Gestión de Servicios de Tecnologías de la Información, es que le sirva como marco de referencia para su desarrollo, de forma que no tenga que "reinventar la rueda", ni en el plano estratégico, la planificación del sistema, ni en el táctico, adopción de "buenas prácticas", y poner en valor dicho marco para la organización, aumentando la eficacia y eficiencia de la misma. Bajo este prisma deben de desterrarse concepciones de épocas pasadas donde la razón de ser del desarrollo de un Sistema de Gestión basado en una norma era la consecución de un sello de acreditación, o el cumplimiento a toda costa de los requerimientos de dicha norma frente al valor que aportaban.

En el sentido anteriormente mencionado, la UNE ISO/IEC 20000:2007-1, proporciona un marco de referencia, suficientemente global y estructurado, para que el desarrollo de un Sistema de Gestión de Servicios TI se pueda realizar de forma que aporte valor al cliente de TI y además, pueda integrarse de forma natural en otros Sistemas de Gestión de la organización basados en otras normas o modelos. Esta parte de la norma respondería a la pregunta: ¿qué debería hacer la organización para la Gestión de Servicios TI? Y la parte 2, UNE ISO/IEC 20000:2007-2, respondería a ¿cómo podría lograrlo?

La estructura de la norma UNE ISO/IEC 20000:2007-1 se basa en 10 cláusulas:

1. Alcance.
2. Términos y definiciones.
3. Requerimientos para un Sistema de Gestión.
4. Planificación e implementación de la Gestión de Servicios.
5. Planificación e implementación de servicios nuevos o modificados.
6. Proceso de prestación de servicio.
7. Procesos de relaciones.
8. Procesos de resolución.
9. Procesos de control.
10. Proceso de liberación.

En la temática que nos ocupa, la Seguridad de la Información, dentro de la cláusula 6, se establece la sub-cláusula 6.6 Gestión de la Seguridad de la Información. En dicha sub-cláusula, se hace referencia explícita a la ISO/IEC 17799 como guía para la Gestión de la Seguridad de la información que, como es sabido, hace referencia a los controles de seguridad de la información o código de buenas prácticas.

Atendiendo a lo que especifica la norma en este punto, se establece como punto de partida la aprobación de la política de seguridad de la organización por parte de la dirección de la organización como guía del proceso y, por tanto, debe ser comunicada a los grupos de interés implicados.

De igual forma, y siguiendo el mismo esquema que se puede observar en normativas relativas a Sistemas de Gestión de Seguridad de la Información, se establecen una serie de requerimientos que deben desarrollarse mediante controles específicos y documentados, entre otros y sin ser exhaustivos, para la implementación de los requisitos descritos en la política y la gestión de riesgos. Debe evaluarse el impacto de los cambios en la organización sobre los controles previamente a su implementación. Deben formalizarse los requisitos de seguridad cuando se precise la accesibilidad de grupos de interés externos a sistemas o servicios prestados y deben gestionarse, en su amplio sentido, los incidentes de seguridad mediante procedimientos que permitan su tratamiento, comunicación y registro. Y por último, y muy importante, las acciones de mejora identificadas durante el proceso de gestión de la seguridad de la información deben incorporarse como entradas del plan de mejora de servicios TI.

El desarrollo de este sub-apartado 6.6 de la norma, se puede realizar en base al desarrollo de un sistema de seguridad de la información, basado en otra normas o estándares, como podría ser la ISO/IEC 27001:2005. Por tanto, cualquier esfuerzo que la organización haya hecho en este sentido podrá ser aprovechado de acuerdo con la filosofía anteriormente descrita de marco de referencia.

Así pues, la ISO/IEC 20000:2005, pretende salvar el *gap* existente, en muchas organizaciones, entre la Gestión de Servicios TI y la gestión de negocio, con la visión holística de hacer que los servicios TI añadan valor a los procesos de operativos o de negocio de la organización con la finalidad de aportar valor en el servicio prestado al cliente final.

4. Referencias

- ISO 17799
- COBIT
- ISO 27001
- UNE 71502
- BS7799-2
- ITIL
- PMI

5. Bibliografía

- BS 25999-1:2006 *Business Continuity Management* – Part 1: *Code of Practice.*

- Página Web de la Agencia de Protección de Datos - https://www.agpd.es/

- Ley Orgánica 5/1992 de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal. (LORTAD)

- Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal. (LOPD).

- Reglamento de Medidas de Seguridad Real Decreto 994/1999, de 11 de junio.

- Página web del Ministerio de Industria, Turismo y Comercio. http://www.lssi.es

- PMI, *Project Management Institute* – www.pmi.org

- ITIL, *Information Technology Infraestructura Library*. http://www.itil-officialsite.com/

- ISO 27001.

Gestión estratégica de seguridad en la empresa

anetcom

C/ Luis Vives 6, 4º, 12ª
46003 Valencia
Tel. 96 392 39 16
Fax 96 392 40 83
informacion@anetcom.es
www.anetcom.es

GENERALITAT VALENCIANA
CONSELLERIA D'INDÚSTRIA, COMERÇ I INNOVACIÓ

Colabora:

CSIRT-CV
Centre de Seguretat TIC de la Comunitat Valenciana