Análisis de Riesgos en la Agencia Estatal de Meteorología mediante el empleo de Magerit y PILAR

Julio González Breña
Responsable Técnico de Seguridad
Jefe del Servicio de Seguridad de Sistemas de Información
Agencia Estatal de Meteorología

PALABRAS CLAVE:

Meteorología aeronáutica, seguridad, protección, ISO 17799, riesgos, Magerit, PILAR, análisis, salvaguardas.

1. SISTEMA DE GESTIÓN DE LA PROTECCIÓN:

La Agencia Estatal de Meteorología (AEMET) tiene por misión cubrir la demanda social de información meteorológica mediante la prestación de servicios que contribuyan a preservar vidas humanas, bienes materiales y el medio ambiente. Para ello debe dotarse de las capacidades necesarias, tanto organizativas como científicas o tecnológicas.

En el entorno de empleo de sistemas abiertos, redes de comunicaciones, bases de datos y publicación electrónica de la información, el desarrollo de cualquier actividad provoca en los procesos de negocio una progresiva dependencia tecnológica. En la actualidad, es esencial garantizar no sólo la continuidad de tales procesos, sino la seguridad, validez y eficacia de las transacciones realizadas y la protección de la información gestionada.

En los últimos años, la AEMET ha abordado un camino hacia la modernización de sus procesos de trabajo, en parte como resultado de la aplicación de compromisos legales y obligaciones con terceros. El Sistema de Gestión de la Protección (SGP) constituye el elemento central sobre el que pivota la seguridad del personal, las instalaciones y la información en la AEMET. Dentro de él se incluyen su compromiso con la seguridad, plasmado en la política de seguridad, la estructura organizativa y asignación de funciones y responsabilidades, así como el conjunto de documentación que facilita su implantación.

2. ALCANCE:

El objetivo marcado para el proyecto fue incrementar la seguridad mediante el mantenimiento de la integridad, disponibilidad, confidencialidad y control de los sistemas informáticos y de la información manejada y depositada en ellos. La integridad asegura la inalteración, la disponibilidad supone permanente estado de operatividad y la confidencialidad implica que sólo entidades autorizadas están en situación de proceso de la información. El control sólo es posible cuando ciertos usuarios definen reglas que establecen el medio y condiciones de acceso para el resto de usuarios de la organización.

En paralelo se intentaba reforzar la seguridad física de las instalaciones y la protección del personal, mejorando simultáneamente la continuidad de los servicios de mantenimiento. Para lograr estos objetivos se ha avanzado en la reducción de la frecuencia de fallos y en la mejora de la capacidad de respuesta ante los mismos.

Con este planteamiento, se definiría el **alcance** del proyecto como:

> Desarrollo e implantación de un Sistema de Gestión de la Protección de la seguridad física y lógica de acceso a las instalaciones, personal y datos operacionales implicados en la recepción, elaboración, operación y transmisión de la **información meteorológica aeronáutica** de la Agencia Estatal de Meteorología.
>
> En consecuencia, el SGP incluye las **normas** y **procedimientos** de mitigación de riesgo y mejora de la seguridad de los activos implicados, así como la emisión de alertas y puesta en marcha de medios de contención.

Es preciso señalar que la AEMET cuenta con una distribución territorial de sus funciones, de forma que la generación de productos y servicios meteorológicos se encuentra lo más cerca posible de los usuarios finales a los que están destinados. El SGP tendría que implantarse especialmente en las siguientes unidades operativas:

- 44 Oficinas Meteorológicas de Aeródromo (OMA) y Oficinas Meteorológicas de Defensa (OMD) abiertas a tráfico civil.
- 11 Grupos de Predicción y Vigilancia (GPV), en sus funciones como Oficinas Meteorológicas Principales Aeronáuticas (OMPA) y Oficinas de Vigilancia Meteorológicas (OVM de Las Palmas).
- Centro Nacional de Predicción, incluyendo sus funciones de OVM.
- Centro de Proceso de Datos (CPD).

De forma análoga el SGP tendría que implantarse en el resto de unidades de la AEMET que sirven de apoyo a la prestación de servicios aeronáuticos (15 Centros Meteorológicos Territoriales; Área de Observación; Área de Comunicaciones, Seguridad y Gestión de Datos; Servicio de Aplicaciones Aeronáuticas, etc.)

3. METODOLOGÍA APLICADA:

Para la construcción del Sistema de Gestión de la Protección se han tenido muy especialmente en cuenta los requisitos aplicables de las Normas siguientes:

- **Reglamento (CE) nº 2096/2005**, que establece los Requisitos Comunes para Prestación de Servicios de Navegación Aérea.
- **UNE-ISO/IEC 17799**: Código Buenas Prácticas para la Gestión de la Seguridad de la Información.

Como referencia, también se han utilizado además las siguientes normas:

- **UNE 71502**: Especificaciones para un Sistema de Gestión de Seguridad de la Información. Describe los pasos a dar para el establecimiento, implantación, documentación y evaluación de un SGSI
- **UNE 71501**: Guía para la Gestión de la Seguridad de las Tecnologías de la Información.

Para el desarrollo y planificación del análisis de riesgos se ha seguido:

- **Magerit versión 2** (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de las Administraciones Públicas), elaborada por el Consejo Superior de Administración Electrónica.
- **PILAR** (Procedimiento Informático y Lógico del Análisis de Riesgos) versión 3.3 (10-03-2007). Se ha utilizado tanto para la valoración de activos, como para la de amenazas y la estimación del riesgo potencial.

Magerit se adoptó como el método formal para analizar los riesgos que soportan los Sistemas de Información, y para recomendar las medidas apropiadas que deberían adoptarse en la mejora de su control. Proporciona un número razonable de herramientas para ofrecer un mapa de los riesgos a que está sujeta la organización en el ámbito del proyecto, simplificando considerablemente la recogida de los datos precisos para la toma de decisiones.

En función del marco normativo, y sin entrar en demasiados detalles, puede asumirse que el esquema sobre el que finalmente se construye el SGP es el clásico **PDCA**, que se resume en la figura 1.

Fig1: Ciclo del Sistema de Gestión de la Protección

4. POLÍTICA DE SEGURIDAD Y ESTRUCTURA ORGANIZATIVA:

Para la organización de la seguridad es imprescindible contar con una serie de documentos que indiquen a los distintos actores cuales son los objetivos de la organización y que responsabilidad y funciones desempeña cada uno.

La base del SGP y de la protección en su conjunto es la **Política de Seguridad**, y mediante su aprobación la AEMET expresa su compromiso con la seguridad y pone de manifiesto las líneas generales que permitirán alcanzar las metas propuestas. Este documento debe ser publicado y comunicado, de forma que sea accesible a todos los empleados de la institución. Además, en la propia Política de Seguridad se hace una mención expresa al SGP, al manifestar lo necesario de su planificación y la importancia que su implantación tiene para la AEMET.

Como segunda piedra angular se cuenta con el **Manual de Organización y Gestión de la Seguridad de la Información, las Instalaciones y el Personal**, un documento en el que, en base a lo dispuesto en la Política de Seguridad, se establece el organigrama de la seguridad y se asignan responsabilidades y funciones a los distintos actores encargados de su implementación.

Los nombramientos de los integrantes de la estructura de personal, son realizados por el Director General de la AEMET, e implican que quienes los reciben pasan a formar parte del **Comité de Coordinación de la Seguridad** (CCS). El CCS controla el funcionamiento del sistema y la elaboración y revisión de normas de seguridad. Sus miembros pueden promover la creación o modificación de normas de seguridad para garantizar la disponibilidad, integridad y confidencialidad de los activos de información y la protección del personal y las instalaciones ante actos de interferencia ilícita.

5. ANÁLISIS DE RIESGOS; MAGERIT Y PILAR

Tradicionalmente se considera que el análisis de riesgos es fundamental para la gestión de la seguridad de los sistemas de información. Mediante su aplicación, se obtiene información acerca de los activos, la valoración del impacto que para la organización puede suponer la pérdida de los mismos y la identificación de las amenazas a las que están expuestos. Por tanto, el análisis constituye el núcleo central de toda actuación organizada y sistemática en materia de seguridad para mejorar la gestión global del riesgo. Es lógico que así sea, ya que los resultados obtenidos acaban influyendo en la estrategia de la organización (por ejemplo mediante cambios en la política de seguridad) y en la realización de mejoras concretas, sobre todo a través de la implantación de salvaguardas.

Sobre la base de las decisiones iniciales tomadas y con el apoyo de la estructura definida, fue posible iniciar la gestión de riesgos mediante la identificación de los mismos y la reducción de su frecuencia de aparición y de los daños que causan. En el proyecto emprendido, se ha situado la gestión del riesgo en el centro de las acciones a emprender, considerándolo la piedra angular de toda la actuación realizada. Sus resultados, particularmente en una primera fase, han sido esenciales para la gestión global de la seguridad que se ha llevado a cabo.

La aproximación metódica es la única posible, si se pretende que el análisis sirva de soporte a la inevitable toma de decisiones. Como se ha indicado con anterioridad, en el caso de la AEMET se optó por aplicar la metodología Magerit para se realización. Las fases seguidas fueron:

- Recogida de información.
- Identificación de los activos relevantes.
- Valoración de los activos.
- Determinación de las amenazas potenciales sobre cada activo.
- Identificación del grado de vulnerabilidad de cada activo a las amenazas que le afectan.
- Estimación del impacto sobre el activo de la materialización de la amenaza.
- Medida del riesgo, analizando el impacto ponderado por la frecuencia de ocurrencia de la amenaza.

Puesto que el empleo de Magerit es complejo y prácticamente imposible de realizar a mano cuando el número de activos es relativamente grande, se justifica la necesidad de disponer de una ayuda en forma de herramienta de soporte. Además, el inevitable mantenimiento futuro, necesario para la propia organización y para una hipotética certificación, con cambios en el inventario de activos y en la naturaleza de los mismos, impone la adopción de una herramienta que automatice la generación de sucesivas versiones.

La herramienta elegida ha sido PILAR, que ofrece un amplio conjunto de utilidades para la realización de un análisis cualitativo, como el llevado a cabo en la AEMET. Gracias a PILAR ha sido relativamente sencillo sistematizar el proceso laborioso de carga de datos y calcular con posterioridad los impactos y los riesgos. Los resultados obtenidos por la propia herramienta aportan una versión simplificada de la complejidad del problema, mediante la que es posible comprender mejor el mismo y adoptar conclusiones razonadas.

Como punto de partida para la realización del análisis, se efectuaron 25 entrevistas con diversos responsables de la AEMET, generando a continuación un acta que se remitió a cada uno de los entrevistados para que tuvieran oportunidad de corregir posibles errores de interpretación o matizar las cuestiones que consideraran adecuadas. Además, se encuestó a los Directores de CMT (15) y Jefes de OMA (44).

Mediante el análisis de la información recogida, se identificaron más de **230 activos** directamente relacionados con la aeronáutica, considerando, por ejemplo, que el conjunto de sistemas de información iguales instalados en oficinas diferentes constituyen únicamente un activo. A continuación, los activos definidos se agruparon en cinco capas diferentes en función de su naturaleza. Para su valoración se tuvo en cuenta la importancia dada por los entrevistados a los servicios en disponibilidad, integridad y autenticidad de los usuarios del servicio y de quien accede a los datos.

En base a los datos obtenidos y al análisis de la organización, se realizó una asociación de dependencias para los diferentes activos en el árbol creado. A continuación, asignando un rango de valoración de 0 a 10 para cada dimensión y activo, y considerando las relaciones de dependencia definidas con anterioridad, se construyó el **Modelo de Valor**.

Tomando como referencia el conjunto de amenazas previstas para cada activo por la herramienta PILAR y considerando la opinión y experiencia de los usuarios, fue posible determinar la frecuencia de materialización de una amenaza (modelada con una tasa anual de ocurrencia) y la medida de la degradación de cada activo. La información se organizó en el **Mapa de Riesgos**.

Para valorar el impacto de la materialización de una amenaza sobre cada activo, se ha tenido en cuenta:

- Impacto acumulado: El valor acumulado de cada activo (su propio valor más el de todos los otros activos que dependen de él) y las amenazas a que está expuesto.
- Impacto repercutido: Se calcula teniendo en cuenta el valor del propio activo y los impactos que resultan sobre los activos de los que depende.

Por último, se realizó una valoración individual del riesgo a que está expuesto el conjunto de activos estudiado. El **riesgo acumulado** se estimó en función del valor de cada activo y sus dependencias, teniendo en cuenta que el impacto sobre un activo produce daños directos sobre ese activo e indirectos sobre los que dependen de él. El **riesgo repercutido** se calculó teniendo en cuenta sólo el valor de cada activo, sin considerar las dependencias.

En resumen, el empleo de la metodología Magerit y la herramienta PILAR en el trabajo realizado ha permitido:

- Mejorar el conocimiento sobre el estado de seguridad de los sistemas de información y las medidas de seguridad asociadas a ellos.
- Sistematizar el estudio, de forma que no haya elementos que permanezcan al margen del análisis, asignando a cada uno la importancia relativa que le corresponde.
- Incorporar mecanismos de seguridad en los propios sistemas de información.

6. GESTIÓN DE SALVAGUARDAS

Una vez identificado y valorado, el primer paso para la gestión efectiva y reducción a un nivel aceptable del riesgo es la **selección de salvaguardas** aplicables. El estudio de las salvaguardas se realizó sobre los riesgos de nivel alto (7), medio (6) o bajo (5). En esta fase de implantación del SGP, el objetivo fue alcanzar un **riesgo residual** (que permanece después de aplicar las salvaguardas y se considera aceptable por la organización en esta fase del proyecto) con un valor inferior a 5.

El proceso de reducción, que puede parecer muy ambicioso, se simplifica cuando, como sucede frecuentemente, una sola salvaguarda sirve para reducir el riesgo que afecta a un amplio conjunto de activos (por ejemplo la existencia de una política de seguridad afectaría a toda la organización y, consecuentemente, reduce de forma simultánea el riesgo del conjunto de activos analizados).

Las **127 salvaguardas seleccionadas** por el Comité de Coordinación de la Seguridad fueron propuestas al Director General, que con su aprobación aceptó implícitamente la existencia de riesgos que no se pueden gestionar en esta fase del proyecto.

El último paso en la gestión del riesgo ha consistido en la elaboración de un **Plan de Mejora**. Dentro de él, se asignó a cada RSA el conjunto de salvaguardas de las que debía hacerse cargo. A su vez, el RSA pudo dividir cada salvaguarda en un conjunto de proyectos o agruparlas con otras. En su ámbito de competencias y para cada proyecto individual definido, cada RSA designó distintos responsables de la ejecución de los proyectos en las fechas previstas.

Además del Plan de Mejora, el SGP cuenta con un procedimiento específico que define los hitos y evidencias que se precisan para el seguimiento efectivo de su aplicación.

El resultado de la aplicación de las salvaguardas se refleja en la figura 4, donde se aprecia la progresiva reducción del riesgo en las fases sucesivas del proyecto y la estimación de la previsible reducción que la aplicación del conjunto de medidas correctivas podría suponer.

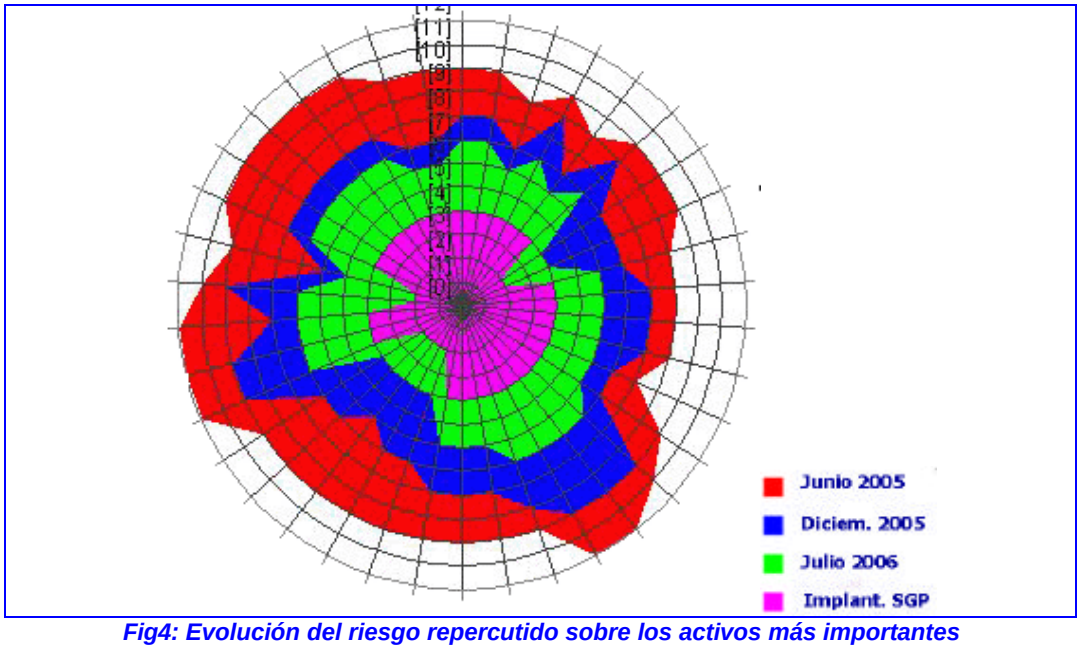

Fig4: Evolución del riesgo repercutido sobre los activos más importantes

La implementación y puesta en operación de **Planes de Contingencia**, fase que se encuentra en desarrollo en la actualidad, constituye el último elemento en la implantación efectiva del SGP. El conjunto de procedimientos de contingencia definidos abarca a todos las unidades de la AEMET que tienen relación con la gestión de información meteorológica aeronáutica. En la mayor parte de ellas se encuentran operativos y están empezando a ofrecer los primeros frutos.

Sin embargo, el campo de aplicación de los planes de contingencia no tiene que limitarse necesariamente a la aeronáutica y, en aquellos casos en que los responsables de las unidades lo han considerado adecuado, se han hecho extensivos a otros ámbitos de la actividad de la AEMET.

7. DOCUMENTOS DEL SGP

El SGP se organiza mediante un nutrido grupo de documentos que contienen las reglas esenciales para su implantación. Cada documento se identifica por la fecha de creación y el número de edición. En aquellos que deben ser firmados, se incluyen las firmas de quién edita, revisa y aprueba el documento. Uno de los elementos esenciales para el acceso a la información del SGP es la definición de un sistema de gestión documental en el que, minimizando la posibilidad de error, sea posible localizar de forma sencilla la versión operativa de cada documento.

Fig5: Página de acceso al portal del SGP

Dentro de la página del SGP, los diferentes documentos que se publican se han organizado en función de su naturaleza:

- **Políticas de Seguridad**: Además del documento general, se incluyen otras 7 políticas sectoriales.
- **Manuales de Seguridad**: Incluyen el propio manual del SGP y el de organización y gestión, así como los manuales de autoprotección (elaborados en aplicación de la normativa vigente de protección de riesgos laborales).
- **Procedimientos de Seguridad**: Definen la aplicación concreta de las medidas generales definidas en las políticas, con un total de 76 documentos.
- **Planes y procedimientos de contingencia**: Describen la forma de actuar ante situaciones de emergencia. Aunque todavía están en desarrollo, ya se han implementado y puesto en operación mediante 6 documentos.
- **Informes del SGP**: Más de 50 documentos, que incluyen todas las salidas específicas del análisis de riesgos (entrevistas, identificación de activos, modelo de valor, mapa de riesgos, estimación del riesgo, propuesta de salvaguardas, plan de mejora, informes de seguimiento de aplicación de salvaguardas, etc.)
- **Otros documentos**: Contratos de suministro, formularios, listados de incidencias, informes de resolución de incidencias, cursos realizados, etc.

8. RESUMEN

La amplitud del análisis a realizar sobre miles de elementos, con más de 230 activos organizados en 5 capas y analizados para cuatro dimensiones, implica una considerable dificultad para la correcta aplicación de Magerit. La complejidad de la propia metodología, el número de activos y las múltiples relaciones de dependencia que pueden establecerse entre ellos, justifica el empleo de una herramienta como PILAR, dado el valor añadido que con su uso puede aportar al proyecto.

La aplicación sistemática de la metodología seleccionada ha hecho posible identificar los activos más críticos para la organización y tener una visión de los riesgos que pueden afectar de forma más grave a la prestación del servicio de datos meteorológicos a la aeronáutica. Debe aceptarse un inevitable grado de subjetividad e incertidumbre sobre el resultado final, que será inversamente proporcional a la calidad del análisis realizado.

El éxito del proyecto se pone de manifiesto en la adopción de numerosas salvaguardas mediante decisiones adoptadas a nivel directivo, que han contribuido a disminuir el nivel de riesgo a que estaba sometida inicialmente la organización.