Sistema de Gestión de la Protección del Instituto Nacional de Meteorología

Julio González Breña
Responsable Técnico de Seguridad
Jefe del Servicio de Seguridad de Sistemas de Información
Dirección General del Instituto Nacional de Meteorología

PALABRAS CLAVE:

Meteorología aeronáutica, seguridad, protección, ISO 17799, riesgos, Magerit, PILAR, incidencias de seguridad, gestión documental electrónica, auditoría

RESUMEN DE LA COMUNICACIÓN

El Instituto Nacional de Meteorología (INM) 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 Dirección General del INM 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. La mejora alcanzada en la seguridad de la información y la protección de su personal e instalaciones, junto a otros proyectos, contribuyó a que en diciembre de 2006 el INM obtuviera el certificado que lo acredita como proveedor de servicios meteorológicos a la navegación aérea.

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 el INM. Dentro de él se incluyen el compromiso de la Dirección General 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.

Una de las mayores dificultades reside en la publicación eficaz de la información intrínseca al sistema y la gestión de las incidencias de seguridad detectadas. Estas últimas deben ser reportadas de forma que lleguen hasta los responsables con nivel administrativo adecuado para su subsanación y además tienen que gestionarse para, mediante el análisis posterior, servir a la adopción de medidas correctivas y preventivas, tendentes a la mejora del propio SGP.

En este trabajo se analiza el esfuerzo organizativo realizado, que incluye un canal de gestión de la documentación, apoyado en la publicación electrónica de la misma desde la página del SGP, y en la utilización de la aplicación Mercurio para la gestión de las incidencias de seguridad.

1. RECURSOS HUMANOS DISPONIBLES PARA EL PROYECTO:

La dirección del proyecto (incluyendo el análisis de riesgos), la elaboración de los documentos de alto nivel (política, manuales, propuesta de estructura organizativa para la seguridad) y la coordinación para la gestión de los riesgos necesaria tras el análisis, son funciones desarrolladas desde un único puesto de trabajo que acabaría recibiendo el nombramiento de Responsable Técnico de Seguridad. Resulta necesario señalar que desde el comienzo de los trabajos se ha contado con el respaldo decidido de la Dirección General y el apoyo organizativo del INM.

El desarrollo del análisis de riesgos ha sido resuelto por la empresa ISDEFE, que además ha dado soporte de consultoría desde su mayor experiencia en este tipo de proyectos.

Una vez finalizado el análisis, la gestión de los riesgos se ha desarrollado con el trabajo colectivo del conjunto de unidades encargadas de la implantación del Sistema de Gestión de la Protección (SGP), incluyendo la redacción de los procedimientos locales de las distintas unidades.

El diseño, creación y desarrollo de los sistemas de gestión documental y de tratamiento de incidencias se logrado con medios propios del INM.

2. CIELO ÚNICO EUROPEO Y NECESIDAD DE CERTIFICACIÓN:

La Comunidad Europea ha desarrollado un conjunto de normas bajo la denominación de Cielo Único Europeo cuyo objetivo es establecer un marco armonizado para mejorar la seguridad y eficiencia del transporte aéreo y aumentar así la capacidad de responder a las necesidades de los usuarios. Este conjunto normativo afecta, entre otros, a los proveedores de servicios a la navegación aérea, entre los que se encuentran los servicios meteorológicos.

La aplicación de esta normativa en España ha dado lugar a la creación de la figura de la Autoridad Nacional de Supervisión de los proveedores de servicios meteorológicos a la navegación aérea, siendo asumidas estas funciones por la Secretaría General para la Prevención de la Contaminación y el Cambio Climático.

La legislación europea obliga a los proveedores de servicios a obtener la acreditación o certificación correspondiente expedida por la Autoridad Nacional de Supervisión, previa comprobación de que cumple con el conjunto de requisitos comunes establecidos.

El Instituto Nacional de Meteorología, como prestador de servicios meteorológicos a la navegación aérea, ha tenido que abordar el complejo proceso de adaptación a la normativa común europea que le permitiese obtener el certificado correspondiente. El proceso de certificación implica la comprobación del grado de adaptación a los requisitos exigidos mediante un conjunto de auditorías realizadas por la ANS. En lo tocante a la seguridad, mediante dichas auditorías periódicas se pretende confirmar que el SGP ha sido diseñado de acuerdo a los requisitos establecidos y su grado de implantación real en las diferentes unidades del INM.

3. ALCANCE:

El objetivo del proyecto en los términos expuestos sería 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.

Además, deberían contemplarse medidas para reforzar la seguridad física de las instalaciones y la protección del personal. Al mismo tiempo, es preciso garantizar la continuidad de los servicios de mantenimiento, reduciendo en lo posible la presencia de fallos y mejorando la capacidad de respuesta ante los mismos.

Con este planteamiento, se define 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** del Instituto Nacional de Meteorología.
>
> En consecuencia, 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.

El INM 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 Aeronáuticas Principales (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).

También será necesario garantizar la implantación del SGP en el resto de unidades del INM 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.)

4. 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 establecen 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.

A pesar de que el Reglamento considera solamente como referencia la norma UNE-ISO/IEC 17799, no imponiendo su seguimiento, se ha decidido aplicarla lo más

ajustadamente posible con el objetivo de que sea posible obtener la certificación de la prácticas de seguridad a medio plazo.

Como referencia para la que no se pretende certificación, 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), elaborada por el Consejo Superior de Administración Electrónica.
- **PILAR** (Procedimiento Informático y Lógico del Análisis de Riesgos) se ha utilizado tanto para la valoración de activos, como para la de amenazas y la estimación del riesgo potencial.

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

5. POLÍTICA Y ORGANIZACIÓN DE LA SEGURIDAD:

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 sistema a diseñar es la **Política de Seguridad**, y mediante su aprobación la Dirección General del INM 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, de forma que se manifiesta la necesidad de su planificación e implementación y la importancia que tiene para el INM.

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. Para su redacción se ha tenido como referencia el documento, elaborado por el Centro Criptológico Nacional, CCN-STIC-201 (Organización y Gestión STIC).

Dentro del Manual se agrupan, revisan y describen el conjunto de funciones en relación con la seguridad que se venían desarrollando en el INM. La principal diferencia y la aportación del trabajo realizado consiste en la organización de todas ellas y la adscripción de responsabilidades de forma unívoca, con la posibilidad de delegar únicamente las funciones. En ningún caso se han creado puestos de trabajo, sino que se han reorganizado las funciones existentes en la estructura directiva para favorecer la implantación del SGP.

Los principales papeles definidos pueden resumirse como sigue:

- **Autoridad de Seguridad**: Director General del INM. Aprueba la Política de Seguridad y nombra a los miembros del Comité de Coordinación de la Seguridad (CCS). Responsable máximo de seguridad, puede delegar sus funciones en los Subdirectores Generales, Directores de Centro y Jefes de Área.
- **Responsable de Seguridad** (SGRS): Subdirector General responsable de todas las funciones delegadas por el Director General. Convoca y coordina el CCS, promueve en la práctica la implantación del SGP y vigila la aplicación de políticas y resto de normas.
- **Responsable de Seguridad de Área** (RSA): Subdirector General o Jefe de Área. Responsables de la seguridad en las instalaciones, personal, sistemas e información bajo su ámbito de competencias. Tienen la posibilidad de nombrar administradores de seguridad para asesorarse en cuestiones técnicas.
- **Responsable Técnico de Seguridad** (RT): Asesor técnico del SGRS, es responsable de la coordinación técnica, la redacción de documentos de seguridad de alto nivel y el asesoramiento del CCS. Diseña planes de formación y se encarga de la concienciación de la seguridad mediante el mantenimiento de diversos portales de información.

Estos nombramientos se realizan por el Director General y significan que automáticamente pasan a formar parte de la composición del CCS. El **Comité de Coordinación de la Seguridad** (CCS) resulta el elemento esencial encargado de la vigilancia del funcionamiento del sistema y de 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.

De esta forma, todo el personal del INM se organiza para la implantación del SGP en una estructura con una división funcional clara:

- **Estructura Principal**: Responsable de la aprobación de normas y de supervisar su implantación. Se organiza en torno al Comité de Coordinación de la Seguridad, al que pertenecen todos sus miembros.
- **Estructura Operacional**: Encargada de la implementación y mantenimiento de requisitos de seguridad definidos. Está constituida

por los administradores de seguridad, de sistemas y redes así como por el conjunto de usuarios del INM.

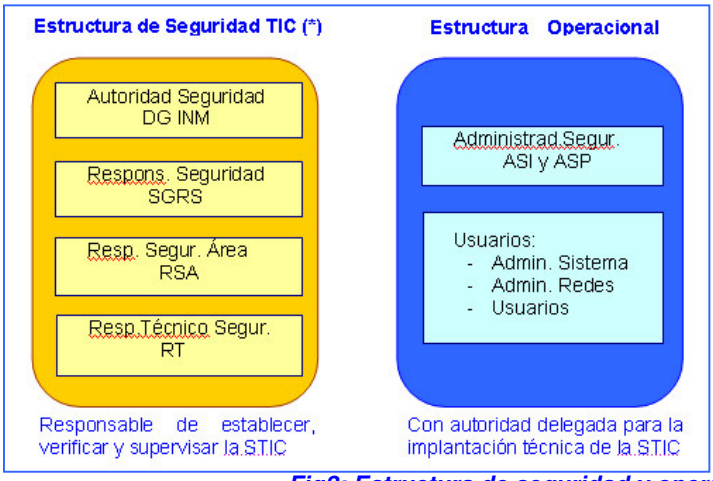

Fig2: Estructura de seguridad y operacional

Como se ha mencionado, los RSA pueden nombrar **Administradores de Seguridad de la Información** (ASI) y **Administradores de Seguridad de las Instalaciones y el Personal** (ASP), para desarrollar las misiones de nivel técnico que el RSA no puede alcanzar y coordinarse con el resto de los actores para la mejora de la seguridad y la identificación de puntos vulnerables en el sistema.

El organigrama de la estructura de seguridad definida sería:

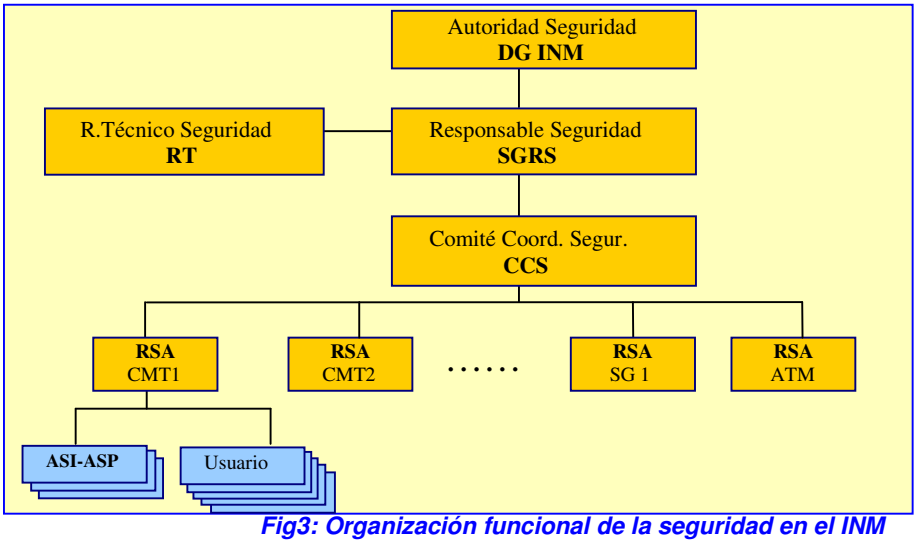

Fig3: Organización funcional de la seguridad en el INM

6. ANÁLISIS DE RIESGOS:

Sobre la base de las decisiones iniciales tomadas por la Dirección General del INM y con el apoyo de la estructura definida, fue posible iniciar el análisis de riesgos. Se trata de una herramienta ideada para la gestión de la seguridad, mediante la identificación de riesgos y la reducción de su frecuencia de aparición y los daños que causan.

Como punto de partida para la realización del análisis, se efectuaron 25 entrevistas con diversos responsables del INM, 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, que se agruparon en cinco capas diferentes en función de su naturaleza. A continuación se realizó una valoración teniendo en cuenta la importancia dada por los usuarios a los servicios en disponibilidad, integridad y confidencialidad. Con esta información se construyó el **Modelo de Valor**.

Tomando como partida 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 y la medida de la degradación de cada activo. La información se organizó en el **Mapa de Riesgos**.

A partir del valor definido con anterioridad, fue posible identificar los activos más críticos para la organización y tener una visión más o menos aproximada a la realidad (el grado de aproximación depende de la calidad del análisis) de los riesgos que pueden afectar de forma más grave a la prestación de servicio.

A continuación 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.

7. SELECCIÓN 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). El objetivo final fue conseguir un **riesgo residual** (que permanece después de aplicar las salvaguardas y se considera aceptable por la organización en esta fase del proyecto) que pudiera considerarse aceptable, 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 reducción que la aplicación del conjunto de medidas correctivas podría suponer.

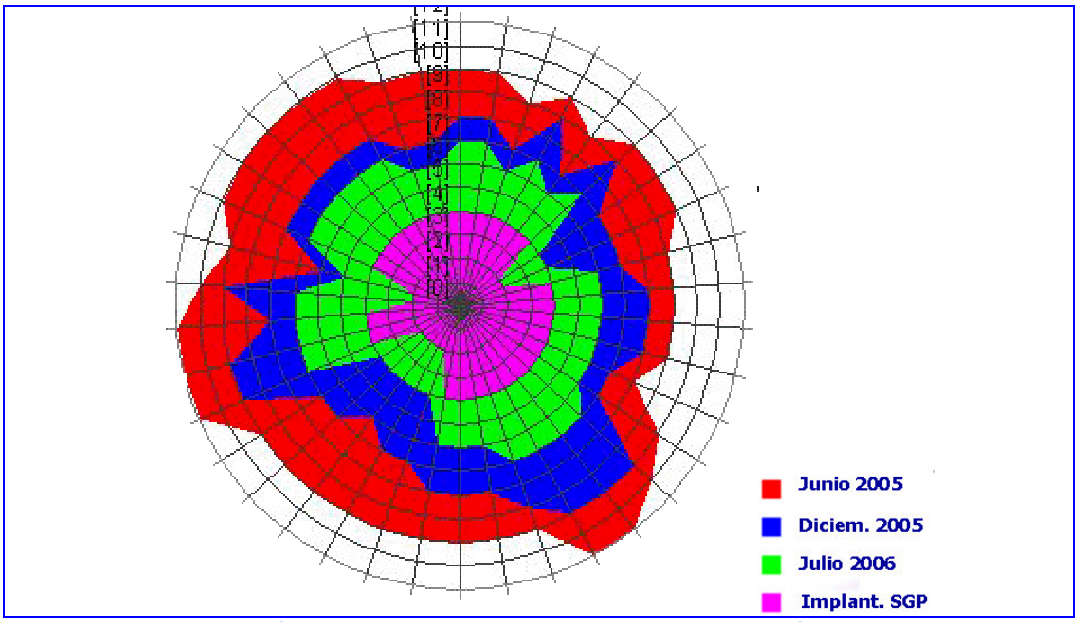

Fig4: Evolución del riesgo repercutido sobre los activos más importantes

El último paso para la implantación del SGP lo constituye la implementación y puesta en operación de **Planes de Contingencia**, fase que se encuentra en desarrollo en la actualidad.

8. SISTEMA DE GESTIÓN DE LA PROTECCIÓN; GESTIÓN DOCUMENTAL

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.

Con ese objetivo, el INM ha decidido la creación de una página web dedicada, que contenga la única versión válida de todos los documentos del SGP. Además, el sistema de gestión documental definido garantiza la copia de seguridad de cada documento en particular, la identificación de las diferentes versiones y el mantenimiento de versiones obsoletas con propósitos legales.

El portal se ha diseñado con diferentes secciones, algunas de ellas reservadas a los RSA y sus administradores de seguridad. Sin embargo, la mayor parte de la información no se encuentra protegida, puesto que el principal objetivo del desarrollo es hacerla llegar hasta los usuarios que deben cumplir lo dispuesto en los diferentes documentos, para así facilitar la comprensión, funcionamiento y estructura del SGP.

Fig5: Página de acceso al portal del SGP

Los diferentes documentos que se publican se han organizado en función de su naturaleza. A través de la página se ha dividido la información en:

- **Políticas de Seguridad**: Además de la Política de Seguridad general de la organización, que debe ser conocida por todo el personal, se incluyen otros 6 documentos de políticas sectoriales para tratar de regular la actividad en campos muy concretos relacionados con la seguridad (de gestión de usuarios, de contraseñas, de acceso a redes, de acceso a aplicaciones y BBDD, antivirus y de instalación y mantenimiento de sistemas).
- **Manuales de Seguridad**: Incluyen el propio manual del SGP y el de organización y gestión.
  Además, es posible acceder a los manuales de autoprotección para las diferentes instalaciones del INM, 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. A su vez se dividen en grupos en función de su naturaleza o las unidades del INM a las que van dirigidos:
  - **Procedimientos Generales**: Afectan a toda la organización, aunque puede que sean aplicados por unidades específicas.
  - **Procedimientos Técnicos**: Desarrollados para sistemas de información concretos.
  - **Procedimientos Locales**: 4 para Servicios Centrales, 15 para Centros y 44 para OMAs.

  El total de procedimientos desarrollados es de 76.
- **Contratos de suministro de servicio**: Los RSA pueden encontrar enlaces a la documentación que sirve de base para la realización de mantenimientos.
- **Informes del SGP**: Más de 50 documentos, que incluyen 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**: Formularios, listados de incidencias de seguridad, informes de resolución de incidencias, cursos realizados, etc.

Una herramienta adicional disponible en la Intranet es la página web desarrollada para ofrecer soporte a la labor técnica que deben realizar los administradores de seguridad y como sistema para difundir información relacionada con la seguridad entre el personal del INM. La portada de acceso a dicha página se presenta en la figura 6.

Fig6: Información técnica sobre seguridad

9. GESTIÓN ELECTRÓNICA DE LAS INCIDENCIAS DE SEGURIDAD

Se considera que una incidencia de seguridad es aquel suceso que pone en peligro el suministro del servicio encomendado a las diferentes unidades del INM o que puede ser síntoma de la existencia de intrusiones ilegítimas en los datos, los sistemas, las instalaciones o hacia el personal.

El registro, análisis y evaluación de las incidencias de seguridad constituye una herramienta esencial para obtener información acerca del estado del Sistema de Gestión de Protección. El análisis de la información obtenida puede servir de base para la toma de decisiones posterior.

En este contexto, es fundamental disponer de un sistema eficaz para la notificación y gestión de incidencias de seguridad que garantice una respuesta rápida, eficaz y ordenada. Para ello se ha diseñado una aplicación, accesible en la Intranet para el personal del INM que en su trabajo tiene relación con la información meteorológica aeronáutica. Existe también una versión en pruebas a disposición de los nuevos usuarios, para que estos puedan familiarizarse con el sistema.

La aplicación Mercurio, cuyo aspecto puede apreciarse en la figura 7, ofrece las incidencias en tiempo real que se generan en cualquier unidad del INM que se encuentra bajo el Sistema de Gestión de la Protección. Las incidencias pueden ser dadas de alta y modificadas a múltiples niveles.

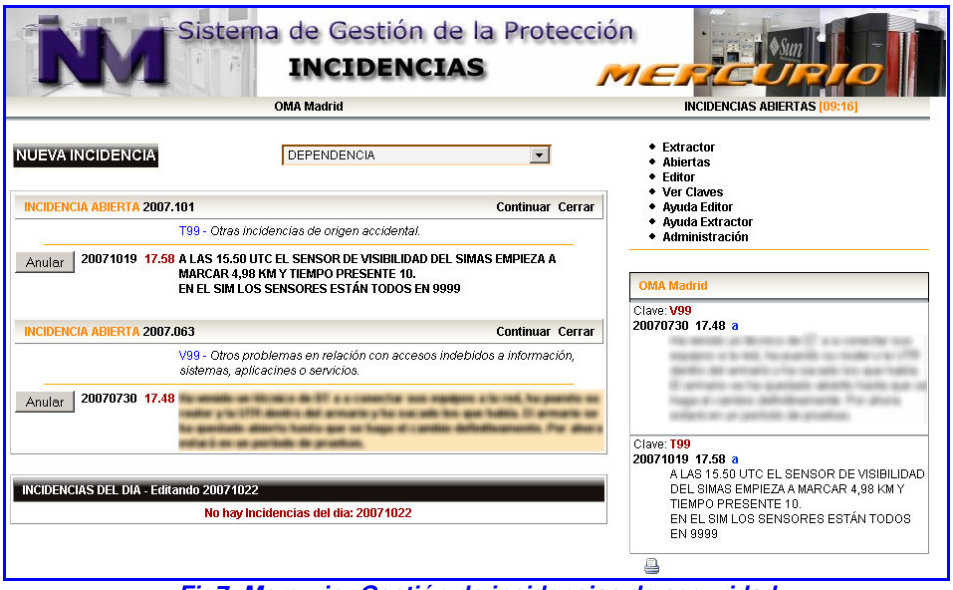

Fig7: Mercurio: Gestión de incidencias de seguridad

Cada unidad tiene acceso a sus propias incidencias, mientras que un RSA puede editar, consultar y anular (no borrar) las incidencias correspondientes a las dependencias de su ámbito de competencias. Por último, tanto el RT como el SGRS pueden acceder al conjunto de incidencias que se generan en el INM. La aplicación dispone de herramientas para la generación de informes, agrupando las incidencias por dependencia, por tipo, en función de palabras clave, etc.

El primer sistema de gestión de las incidencias, basado en la generación de documentos que tenían que conservarse por duplicado, en cada unidad (por ejemplo como evidencia para la superación de auditorías) y además en poder del RSA. En su conjunto resultaba laborioso, complejo de mantener y propenso a la aparición de errores. En la actualidad, aunque todavía en fase preliminar, la implantación de Mercurio contribuye a garantizar el flujo de información sin que sea necesario disponer de documentos de apoyo.

10. FORMACIÓN Y CONCIENCIACIÓN

Un elemento clave para extender la conciencia de la seguridad en el conjunto de una organización es disponer de elementos eficaces para la formación y concienciación de su personal.

El objetivo a conseguir es que los trabajadores del INM dispongan de la información y herramientas suficientes para asumir la responsabilidad y cumplir adecuadamente sus obligaciones, en todos aquellos aspectos relativos a la protección. A largo plazo, se persigue que cada usuario sea consciente de los elementos que facilitan el cumplimiento de los requisitos de seguridad obligatorios para su puesto de trabajo.

Mediante los sucesivos planes de formación anuales, se pretende la difusión de los elementos básicos para la seguridad y la concienciación de los usuarios acerca de las amenazas y riesgos existentes en el ámbito de la protección. El mejor conocimiento de políticas, manuales y procedimientos debe proporcionar un uso racional de los recursos disponibles para la protección de datos, sistemas, instalaciones y personal.

11. RESUMEN

Mediante el SGP, el INM se ha dotado de normas esenciales para la mejora progresiva de la seguridad y la gestión más eficaz del riesgo. El conjunto de políticas, manuales y procedimientos que sirven de base a su aplicación, se mantiene y es accedido desde un portal específico en la Intranet. Además, la gestión de incidencias de seguridad y su posible estudio posterior se apoyan en la existencia de una herramienta que permite consultar la información prescindiendo de documentación de soporte en papel.

Aunque queda mucho por mejorar, es de esperar que el camino recorrido hasta el momento y la apuesta que será necesario realizar para la formación y concienciación del personal, sean los primeros pasos en la adopción de las técnicas más modernas que puedan servir de base a la implantación conceptual de la seguridad.