GOBIERNO
DE ESPAÑA

MINISTERIO
DE TRABAJO
E INMIGRACIÓN

SECRETARÍA DE ESTADO
DE LA SEGURIDAD SOCIAL

GERENCIA DE INFORMÁTICA
DE LA SEGURIDAD SOCIAL

CUMPLIMIENTO DEL ESQUEMA NACIONAL DE SEGURIDAD EN LA SEGURIDAD SOCIAL

Gerencia de Informática de la Seguridad Social
Centro de Calidad, Auditoría y Seguridad
Autor: Pedro C. Valcárcel Lucas.

2010.es
Presidencia Española de la Unión Europea

C/ Dr. Tolosa Latour, s/n
24041 MADRID
TEL: 91 390 27 18
FAX: 91 390 51 67

CUMPLIMIENTO DEL ESQUEMA NACIONAL DE SEGURIDAD EN LA SEGURIDAD SOCIAL

La implantación de la seguridad como una actividad integral es uno de los objetivos fijados hace tiempo en la Seguridad Social. La aprobación del Esquema Nacional de Seguridad ha supuesto un impulso en este sentido, pero también un reto para una gran administración pública, extendida geográficamente, con decenas de miles de usuarios y con gran número y diversidad de activos tecnológicos en sus sistemas de información.

Los primeros pasos

En las últimas dos décadas hemos visto cómo las tecnologías de la información han ayudado a empresas y ciudadanos a disponer de un conjunto muy amplio de servicios de los que hacer uso. Hoy en día por medio de un ordenador se pueden realizar compras, enviar correos y faxes, consultar expedientes, solicitar una cita médica o comprar billetes de avión.

La Seguridad Social no ha sido ajena a estos avances, y ha ido adaptando su oferta de servicios a las tecnologías de la información. Sistemas como RED (Remisión Electrónica de Documentos) fueron unos de los primeros que permitieron hacer las gestiones de afiliación de trabajadores, inscripción de empresas y pago de cuotas a través de nuevas tecnologías y han traído beneficios para la propia organización, con una sustancial reducción de costes derivados del procesamiento manual y una liberación de parte de la carga de trabajo en las oficinas.

Pero también, como ya es de sobra conocido en el mundo de la informática, han aumentado los riesgos de seguridad de la información tratada. Los sistemas intrínsecamente más seguros son los aislados, y la apertura de las administraciones públicas al mundo digital ha supuesto precisamente lo contrario, mayor inseguridad por la naturaleza de los usuarios que acceden a ellos (no sólo internos, sino también externos) y la diversificación de las tecnologías usadas. Por ello desde el año 2004 la Gerencia de Informática de la Seguridad Social (en adelante GISS), organismo que se ocupa del soporte de los sistemas de información ha venido realizando análisis periódicos de riesgos y gestionándolos en planes directores de seguridad y planes de continuidad de negocio. No hay mejor manera de optimizar el nivel de seguridad de una organización que invertir sus recursos técnicos y humanos en los puntos de mayor riesgo.

En paralelo, en esos años la administración pública ha impulsado la aprobación de leyes y normas que dan soporte a la implantación de la administración electrónica, como la conocida Ley 11 / 2007 y

su normativa de desarrollo. En la primera de ellas, el artículo 42.2 establece que la Administración debe aprobar el Esquema Nacional de Seguridad (en adelante ENS) para "establecer la política de seguridad en la utilización de medios electrónicos en el ámbito de la presente Ley, y está constituido por los principios básicos y requisitos mínimos que permitan una protección adecuada de la información.", teniendo presentes las recomendaciones de la Unión Europea en materia de seguridad[1] . Su entrada en vigor, a finales de Enero de 2010, ha marcado el punto de partida para que la gestión de la seguridad se generalice y unifique en todo el ámbito de la administración pública en España.

La gestión como actividad integral

Desde los primeros borradores del ENS, la GISS ha participado en las comisiones de creación del texto y ha colaborado considerando que su contenido sigue los mismos principios que los de los estándares ISO 27001 e ISO 27002, que implementan los Sistemas de Gestión de la Seguridad de la Información (SGSI) y que encajan con varios de los principios que presiden la política de seguridad de la información en la Seguridad Social:

- La proporcionalidad entre las medidas de seguridad aplicadas y el riesgo que reducen.
- La importancia de la seguridad, que viene determinada directamente por los requisitos que exigen los responsables de los servicios que oferta la propia organización, independientemente del entorno informático que les da soporte.
- El análisis y la gestión de los riesgos, que deben realizarse siguiendo las directrices de la administración pública española.

El ENS está constituido por los principios básicos y requisitos mínimos que permitan una protección adecuada de la información.

La mayor de las ventajas del ENS es que declara unos principios y requisitos mínimos comunes a cumplir por cualquier administración, y el más importante de todos ellos desde nuestro punto de vista es que se considera a la seguridad como una actividad integral, en la que no se conciben actuaciones puntuales o tratamientos coyunturales.

[1] (Decisión 2001/844/CE CECA, Euratom de la Comisión, de 29 de noviembre de 2001, por la que se modifica su Reglamento interno y Decisión 2001/264/CE del Consejo, de 19 de marzo de 2001, por la que se adoptan las normas de seguridad del Consejo

Se considera a la seguridad como una actividad integral, en la que no se conciben actuaciones puntuales o tratamientos coyunturales

Cumplimiento del Esquema

Como se ha comentado anteriormente, la GISS ha venido estableciendo medidas para garantizar unos niveles razonables de riesgo en sus sistemas de información. En este sentido ya ha recorrido parte del camino y cumple con los principales requisitos exigidos por el Esquema, pero algunas de sus exigencias van a suponer un esfuerzo considerable de adaptación.

En este sentido es muy importante delimitar el ámbito del cumplimiento, pues no es en general para todos los sistemas, sino para aquéllos con los que el ciudadano interaccione con las administraciones públicas[2] . Para determinar el impacto y las tareas a realizar, en la GISS se ha realizado un análisis y un plan de cumplimiento en el que se establecen por una parte las acciones a realizar para conseguir un sistema de gestión de la seguridad de la información integral y por otra las medidas de seguridad que es necesario completar o implantar.

Este plan se ha desarrollado a partir de una clasificación inicial de los sistemas de información de la Seguridad Social y una asignación de sus requisitos de seguridad en las dimensiones DICAT[3] , que es una base para determinar qué medidas afectan a cada uno de los sistemas.

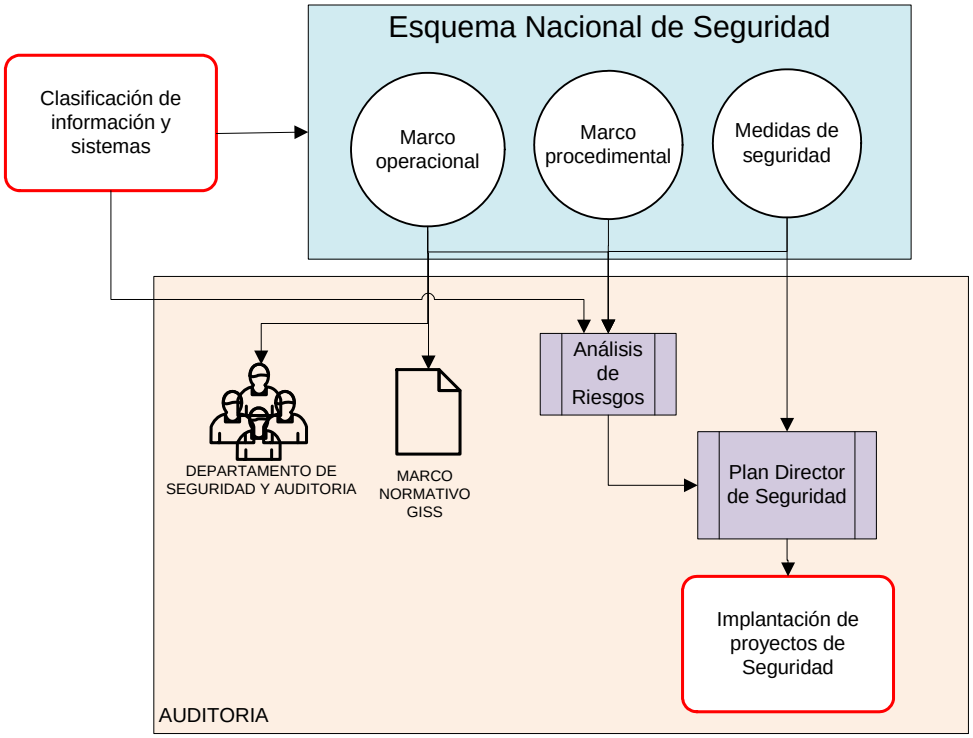
En el ENS las medidas de seguridad a implantar están divididas en tres grandes grupos. En primer lugar están las **medidas del marco operacional**, que hacen referencia a las globales de seguridad que deben ser llevadas a cabo. Entre ellas se incluyen:

- La implantación de la política de seguridad. En la Seguridad Social están desarrolladas pero pendientes de revisión por la dirección.
- El desarrollo de normativas y procedimientos de seguridad. En este punto se han definido y publicado varias normas y procedimientos.
- Los procedimientos de autorización, que en todos los ámbitos están implantados y en muchos formalizados.

[2] Art. 30 del ENS

[3] D=Disponibilidad, I=Integridad, C=Confidencialidad, A=Autenticación, T=Trazabilidad

Estás medidas afectan a todos los sistemas y son el pilar del resto de medidas. En este aspecto la Seguridad Social tiene un largo camino recorrido, aunque quedan pendientes algunos aspectos de formalización.



La GISS está integrando el ENS con nuestros procesos internos de gestión de riesgos

El **marco operacional** está constituido por las medidas a tomar para proteger la operación del sistema como conjunto integral de componentes. Una de las más importantes es la ejecución de un análisis de riesgos periódico. En este sentido, sobre el que ya se está realizando en la GISS, de forma bienal, es necesario ampliar su ámbito para abarcar todos los sistemas de información que estén afectados por el ENS.

El análisis de riesgos es el pilar fundamental de la gestión de la seguridad

Otras medidas de seguridad del marco operacional son también importantes:

- Mecanismos de control de acceso. La Seguridad Social tiene fuertes mecanismos de control de acceso implantados. La conformidad en este punto está muy avanzada.

- Procedimientos de explotación de aplicaciones y sistemas. De nuevo en este punto la Seguridad Social tiene definidos controles y gestión de cambios para la explotación de sistemas y aplicaciones, gracias al esfuerzo realizado en los últimos años.

- Registros de actividad. En la Seguridad Social se dispone de mecanismos que permiten guardar la información de la actividad de los usuarios, así como procesos de gestión de incidencias. El proceso de adaptación en este punto será mínimo.

- Gestión de servicios externos. Estas medidas hacen referencia a la contratación de servicios y la gestión diaria de los mismos, además de garantizar los medios alternativos a los servicios para garantizar los objetivos propuestos. En este apartado la Seguridad Social ha avanzado en los últimos meses, incluyendo el establecimiento y el cumplimiento de los requisitos de seguridad en los pliegos de compras.

- Continuidad de negocio. La Seguridad Social tiene operativo un plan de contingencias basado en la disponibilidad de un centro alternativo de datos. En este apartado debe esforzarse por formalizar los análisis de impacto en el negocio, para que incluyan todos los sistemas objetos del Esquema.

- Especial atención va a requerir adaptar el proceso de desarrollo y compra de equipos y software para asegurar que los componentes esenciales de los sistemas de información estén certificados. Ello supondrá la inclusión de controles de seguridad en esos procesos. El objetivo final será adecuarse de forma gradual a los requisitos establecidos en la materia.

En último lugar, las **medidas de protección** es el grupo más amplio de medidas técnicas aplicables:

- La protección de las instalaciones e infraestructuras. La Seguridad Social tiene bien protegidas sus instalaciones físicas.

- Gestión del personal. El ENS establece algunos requisitos en este sentido, incluyendo algunos aspectos tan importantes como la concienciación, la formación, además de la caracterización de los puestos de trabajo y asignación de responsabilidades. En este punto la Seguridad Social hace tiempo que ha comenzado planes parciales, pero que deben extenderse a todos los ámbitos de los sistemas de información.

- Protección de los equipos. Esta medida hace referencia a la seguridad en los puestos de trabajo fijos y equipos móviles. Las medidas de seguridad ya implantadas deben complementarse para el caso de estos últimos dispositivos.

- Protección de las comunicaciones. Las medidas destacadas en este apartado hacen referencia a medidas que la Seguridad Social ya tiene implantadas en parte de sus sistemas, como definición de perímetros de seguridad, segregación de redes o disponer de medios alternativos, entre otras.

- Protección de los soportes de información. Estas medidas están muy relacionadas con el etiquetado exigible de la LOPD, si bien aquí las referencias son mucho más amplias. La Seguridad Social debe implantar esta medida en muchos de los soportes de información.

- Protección de las aplicaciones informáticas. Incluye medidas genéricas y específicas para la protección de las aplicaciones, tanto en las fases de desarrollo como de puesta en producción. La Seguridad Social ya tiene implantados procedimientos de controles de seguridad en las compras y en los desarrollos propios.

- Protección de los servicios. Al igual que para las aplicaciones, existen medidas de protección para los servicios utilizados, tales como el correo electrónico o servicios web. En esta parte ya existen controles que garantizan la seguridad de los nuevos desarrollos o de las nuevas versiones del software, pero es necesario hacer una revisión exhaustiva de todo el entorno de producción.

Conformidad

El último paso del plan de cumplimiento es lógicamente cumplir con los requisitos de conformidad. En el Esquema se obliga a la ejecución de auditorías, cuyo ámbito y aplicación dependerán de la clasificación de los sistemas realizada. Estas auditorías hacen hincapié en determinar si la administración examinada cumple con los requisitos mínimos y los principios de seguridad determinados en el Esquema.

La auditoría periódica es una parte importante de la implantación del ENS ya que garantiza que la administración ponga especial empeño en la implantación de las medidas.

Conclusiones

El ENS va a suponer en general un paso importante en la mejora de los servicios que la Administración presta a los ciudadanos. En particular en la Seguridad Social consideramos que su cumplimiento, aunque requiera esfuerzos y tiempo, es necesario, razón por la cual desde los mandos directivos ya se ha comenzado a impulsar, convencidos de las ventajas a medio y largo plazo de gestionar adecuadamente la seguridad de la información como un medio de conseguir los fines de la Seguridad Social como una de las administraciones públicas punteras en España.