"Estamos diseñando la arquitectura futura de protección TIC de la Seguridad Social"

Carlos Escudero Rivas,
Director del Centro de Calidad, Auditoría y Seguridad de la Subdirección General de Informática de la TGSS

La Tesorería General de la Seguridad Social ha iniciado uno de los planes más ambiciosos de modernización de protección de la información de los que se tiene noticia en el ámbito de la Administración General del Estado. Sobre esta paradigmática iniciativa habla en la presente entrevista Carlos Escudero, Director del Centro de Calidad, Auditoría y Seguridad de la Subdirección General de Informática de este Organismo, cuya actividad afecta de forma crítica a toda la Seguridad Social y a millones de ciudadanos y empresas.

– ¿Cómo se organiza la seguridad TIC en la Subdirección General de Informática de la TGSS?

– La seguridad informática lleva implantada en lo que ahora constituye la Subdirección General de Informática de la TGSS desde hace más de diez años, cuando su estructura organizativa no era la actual. Hace dos años se creó el Centro de Seguridad, que integra de una forma específica y completa todas las funciones en la materia. Dicho Centro acaba de ampliar sus competencias recientemente a las áreas de Calidad y Auditoría.

– ¿Cuál es su dependencia jerárquica?

– Depende directamente de la Subdirección General de Informática de la TGSS, y está al mismo nivel jerárquico que los otros seis existentes: Adquisiciones, Mantenimiento Evolutivo, Operaciones, Proyectos, Servicios y Tecnología. De hecho, como Director del Centro de Calidad, Auditoría y Seguridad formo parte, junto con los directores de los otros Centros, del Comité de Dirección de la Subdirección General de Informática.

– ¿Se discute mucho sobre seguridad TIC en dicho Comité de Dirección?

– Definimos estrategias y tomamos decisiones que afectan a varios Centros; incluso se informa de las que afectan a uno solo. Obviamente, discutimos sobre todos los asuntos, entre los que se encuentran aquellos que aluden a la seguridad en informática y en comunicaciones. Un ejemplo: las Políticas de Seguridad se llevan al Comité de Dirección y allí se toman las decisiones sobre su ámbito de aplicación e interrelaciones.

– ¿Qué infraestructuras y sistemas dependen, en materia de seguridad de la información y seguridad TIC, del Centro de Calidad, Auditoría y Seguridad?

– La Subdirección General de Informática de la TGSS da servicio también al resto de organismos de la Seguridad Social. Además, y en virtud de la legislación vigente, y a través de nuestro producto propio SILCON, que data de 1991 y que ha registrado una única revisión hasta la fecha, proporcionamos el sistema de confidencialidad a todos los organismos de la Seguridad Social.

Por esa razón, y apoyándonos precisamente en la legislación de referencia, que tiene rango de Real Decreto, hemos realizado una propuesta de Políticas de Seguridad, que en principio queremos probar en esta Subdirección. Una vez concluido este hito, las llevaremos a la Comisión Técnica, en la que existe firma delegada de los Directores Generales de los distintos organismos de la Seguridad Social, para que se aprueben allí y se apliquen a todo el personal de la Seguridad Social.

En otros ambitos de la seguridad, el Centro se hace cargo de productos instalados en la propia Subdirección General de Informática; aunque, cuando otros organismos van a definir arquitecturas o consideran oportuno emprender nuevas aventuras tecnológicas, siempre nos consultan, y a veces nos solicitan que llevemos a cabo una adaptación o desarrollos específicos para distintas finalidades de protección TIC. En suma, que aunque la dependencia del Centro de Seguridad es de la Subdirección General de Informática, sí sin embargo tiene capacidad para influir en el resto de organismos de la Seguridad Social.

– Por su respuesta se deduce que además de los aspectos de planificación y de organización de la seguridad, el Centro realiza también trabajos de desarrollo tecnológico…

– De los tres Grupos que forman parte del Centro, Calidad, Auditoría y Seguridad, el más numeroso es el dedicado a la Seguridad, conformado actualmente por unas cuarenta personas. Este Grupo tiene equipos especializados en distintas áreas: Estrategia, que incluye análisis de riesgos, políticas y difusión de la seguridad; Arquitecturas de Seguridad, que está especializado en participar en los nuevos proyectos que desarrolla la Subdirección General de Informática, para definir sus arquitecturas de seguridad o adaptarlas a las existentes; Mantenimiento, encargado de SILCON; y Administración de la Seguridad, responsable de la administración de la seguridad en la Subdirección General de Informática y de la administración de algunos aspectos concretos no delegados de la seguridad del resto de los organismos de la Seguridad Social.

– ¿Desarrollan labores de prescripción?

– Una de nuestras responsabilidades consiste en asegurar que las herramientas encajen en las arquitecturas tecnológicas existentes. A los efectos oportunos, el Centro de Tecnología es el que diseña las arquitecturas y tiene la visión para evolucionarlas a futuro. Nosotros tenemos ese cometido en lo que concierne a la seguridad. En román paladino: el Centro de Tecnología está encargado de definir cuál va a ser el horizonte de futuro de nuestras arquitecturas tecnológicas, en las que las arquitecturas de seguridad van a ser piezas esenciales; esas arquitecturas de seguridad son responsabilidad del Centro de Seguridad, incluidos los productos de desarrollo propio y los de mercado. Una precisión: las iniciativas de seguridad siempre están dirigidas por profesionales internos especializados en la dirección de proyectos.

– ¿Prevé la creación de nuevos equipos en el Grupo de Seguridad?

– Creo que sí, ya que aunque estamos actualmente mensurando la posibilidad de delegar algunos aspectos de la seguridad técnica, quizás nuestras concepción de la protección de la información aconseje no seguir este camino.

– ¿Hay sinergias reales en el Centro entre la calidad, la auditoría y la seguridad?

– Por supuesto. Para mí, como director, ha sido una gran ayuda y un descubrimiento la incorporación en el mismo Centro de la Calidad; aunque en principio este Grupo está centrado en ámbitos distintos a los de seguridad, como son la descripción de los procesos de la organización, su adaptación y cambio, los vínculos son más que evidentes, entre otras razones porque la seguridad no es un producto, sino un proceso. La seguridad, ciertamente, es un ciclo continuo.

Gracias a esta sinergia, estamos poniendo un foco importante desde el Grupo de Seguridad en el seguimiento de la ISO UNE 17799, para que las acciones que vayamos acometiendo estén encuadradas con su esquema, entendiendo que el mismo hay que adaptarlo de forma correcta a las características de nuestra organización.

En lo referente a la Auditoría, un Grupo como quien dice recién creado, su relación con la calidad y la seguridad es más que evidente. El ciclo de auditoría es, al igual que los de calidad y seguridad, continuo. Pretendemos orientarlo hacia la auditoría informática en general, contexto en el que se incluirá la auditoría de las "seguridades".

"Sería interesante poder aprovechar la experiencia de integradores y fabricantes en la implantación y desarrollo continuo de sistemas de análisis y gestión de logs con fines de seguridad".

– ¿A qué se refiere cuando dice que el esquema de la ISO UNE 17799 hay que adaptarlo a las características de su organización?

– A que el peso concreto de las distintas áreas que se especifican en la ISO UNE 17799 depende de las finalidades y cometidos de la entidad en la que se está realizando el seguimiento de la norma.

– ¿Tienen en desarrollo un plan director de seguridad?

– Como procedemos de una organización muy tecnológica, lo primero que impulsé en el Centro de Seguridad fueron aquellos asuntos menos tecnológicos, tales como la elaboración de políticas, y el análisis y la gestión de riesgos. Entroncado directamente con el proceso permanente de análisis y gestión de riesgos, estamos concibiendo un Plan Global de Seguridad, que constará de una pléyade de proyectos encaminados a corregir y minimizar vulnerabilidades.

Esta iniciativa es fundamental para poder ofrecer a la dirección una imagen clara, breve, concisa, e incluso gráfica, del estado del arte en un momento dado de nuestra organización en materia de seguridad técnica, y de cuánto puede costar pasar de ese estado de seguridad a otro superior. Una pretensión así requiere la creación de un cuadro de mando, para lo que es menester fijar variables e indicadores adecuados.

– No obstante, hay proyectos cuya ejecución no conviene postergar.

– Efectivamente; hay iniciativas que estamos acometiendo, al entender que nuestro propio Plan Global de Seguridad las va a poner de manifiesto más pronto o más tarde. Uno de los proyectos, hoy en fase de prototipo, es el de Tarjeta del Empleado, que cubriría el fichaje en la entrada, la identificación al puesto de trabajo, el bloqueo del puesto de trabajo y otras funciones de certificación electrónica: firma, integridad y cifrado. En principio, se realizará un despliegue entre un grupo específico de la Subdirección General, después se ampliará a todo su personal y a Servicios Centrales, y finalmente se desplegaría en todo el territorio nacional.

– ¿Qué relaciones tiene la Tarjeta del Empleado con el proyecto PROS@?

– PROS@ es una nueva arquitectura de sistemas y aplicaciones muy innovadora, basada en múltiples capas. Ha sido concebida desde el principio para requerir mecanismos como navegadores, arquitecturas Java2, uso de los grandes ordenadores como servidores de datos... En el Centro, y a los efectos del PROS@, colaboramos internamente en el desarrollo de la capa de seguridad a medida para este tipo de arquitecturas. El de Tarjeta del Empleado, que es un proyecto principalmente de identificación/autenticación independiente, complementa a PROS@ en varios frentes. Por ejemplo, a partir de que dispongamos de las funciones de certificación electrónica, podremos añadir en el *workflow* en el que van a estar integrados los procesos de gestión afectados por PROS@, pasos muy interesantes, como el de la firma de documentos.

– ¿Tienen definida la estructura PKI de la TGSS, a efectos de presente y de futuro?

– Disponemos de una PKI en la que se prevé la ampliación de ramas para distintos usos futuros, teniendo en cuenta que siempre se utilizará en el contexto de usuarios propios de la Seguridad Social, y nunca en el papel de tercero de confianza entre dos o más entidades.

– ¿Cuántos certificados electrónicos han emitido en el contexto del Sistema RED?

– En tres meses, 72.000. Lo previsto. Era sencillo calcular el alcance, puesto que conocíamos la población de usuarios. Estamos francamente satisfechos con el Sistema.

– ¿Qué otros proyectos de seguridad están acometiendo?

– Varios, además del de Tarjeta del Empleado. Hay uno que merecen especial atención por su alcance: el de *single sign on*, que aportará comodidad a los usuarios y reforzará la seguridad de gestión de identidades y administración

de usuarios. Más adelante tenemos planificado acometer una iniciativa crítica: la de gestión y análisis de *logs*, cuyas fases están prácticamente definidas.

– ¿Qué autenticador tienen seleccionado para el proyecto de *single sign on*?

– Estamos diseñando la arquitectura de seguridad TIC del futuro, por lo que la pregunta que me hace aún no la puedo contestar de forma categórica. Una de las ideas que barajamos, y que no es independiente del Centro de Seguridad, aunque si es muy sensible al modelo que se fije de arquitectura de seguridad de nuestra organización, es utilizar certificados electrónicos como identificadores.

– En relación con el proyecto de análisis y gestión de *logs*, ¿contemplan el desarrollo interno de herramientas tecnológicas o usarán productos comerciales como base de la solución?

– Tenemos muy claro lo que queremos. En la medida de lo posible vamos a usar herramientas de mercado, si entendemos que tienen la calidad requerida y si está garantizada su evolución según las necesidades de nuestros sistemas. Lo que pasa es que para sacar todo el jugo a estas herramientas, se necesita integrar componentes. Por tanto, además de la experiencia propia, que es amplia y profunda, sería interesante poder aprovechar la de integradores y fabricantes en la implantación de sistemas de análisis y gestión de *logs* con fines de seguridad.

– ¿Tienen un plazo para iniciar este proyecto?

– Nos gustaría abordarlo en 2004, aunque hago hincapié en que se desarrollará por fases.

– En el conjunto de responsabilidades específicas del Centro de Calidad, Auditoría y Seguridad, ¿se encuentran las concernientes a la disponibilidad de sistemas, aplicaciones y servicios?

– Nuestra oganización es muy fuerte en misiones de producción, y en la prestación de servicios con base en la tecnología, por lo que siempre se ha valorado grandemente la disponibilidad, que es la gran olvidada de la seguridad. ¿Cómo estamos enfocando este epígrafe de la seguridad? Pues a partir de las Políticas, hemos creado una serie de documentos, entre los cuales se encuentra el Plan de Contingencias. Dicho plan se ha definido como un proyecto global de la Subdirección General de Informática en el que interviene el Centro de Seguridad como uno más.

– ¿En qué fase se encuentra el proyecto de autorespaldo entre los centros de Orcasitas y Torrejón?

– Profesionales del Centro de Seguridad están colaborando en este complejísimo proyecto, que se está desarrollando por fases, al que se da en la Subdirección General de Informática una importancia capital. La pretensión final es disponer de respaldo mutuo en caliente. Obviamente, la disponibilidad está actualmente garantizada con sistemas en alta disponibilidad, políticas de *backup*, librerías virtuales y salvaguarda de datos en silos remotos seguros.

– ¿Existe una política en virtud de la cual no pueden tomarse determinaciones en materia de seguridad con base tecnológica sin contar con la intervención de Centro de Calidad, Auditoría y Seguridad?

– Sí, claro está; se nos requiere tanto desde la dirección de proyectos para dar forma a párrafos en pliegos en el curso de proyectos cerrados sobre productos cerrados, como para participar en desarrollo de proyectos en el aspecto de seguridad.

"Para el Centro ha sido crucial la independencia frente a otras áreas de la función informática, ya que nos está permitiendo dar una visión homogénea a la seguridad TIC en el contexto de la Seguridad Social"

– ¿Cuál es en su opinión el gran reto que tiene hoy sobre la mesa un gestor de seguridad TIC?

– El de la concienciación de los usuarios. Creemos firmemente que no por disponer de las mejores herramientas tecnológicas el problema de la protección de la información está solucionado; antes bien, hay que tener concienciadas e informadas a las personas acerca de cómo les afecta la legislación, de qué tipo de procedimiento tienen que abrir ante tal o cual incidencia de seguridad... Estamos esperando a que exista una aprobación de nuestras Políticas en la Comisión Técnica para emprender un Plan de Concienciación de Usuarios. Debido a nuestra gran dimensión, para garantizar una buena penetración de este Plan habremos de diseñar una logística y tendremos que formar a profesionales que, a su vez, puedan formar al resto de personal. Igualmente usaremos nuestra Intranet para divulgar noticias de seguridad y para informar acerca de nuestras políticas y procedimientos. Todos los medios son pocos.

– En tanto que directivo de seguridad TIC, ¿considera a la LOPD y al Reglamento de medidas de seguridad aliados o enemigos?

– Tengo sensaciones encontradas. Desde principios de la década de los noventa hemos trabajado mucho en esta Casa para adaptarnos a la legislación sobre protección de datos personales. Además, nuestras relaciones con la Agencia de Protección de Datos son excelentes.

No obstante, creo que hay algunos aspectos tecnológicos introducidos en la LOPD y en el Reglamento que deberían ser revisados por el legislador. Expertos hay que sostienen que si se dispone de datos personales de nivel alto, no sería legal reutilizar los mismos soportes de disco en los que estuvieron almacenados.

En una instalación de la envergadura de la nuestra, esto acarrea una complejidad y un coste añadido poco menos que inasumibles. Es un ejemplo.

– ¿Qué opina del proyecto del DNI electrónico de la Dirección General de la Policía?

– Que es importantísmo. Tenemos con el DNI una ventaja sobre casi todos los países del mundo, ya que es un identificador reconocido que no se discute. Llevar esta condición a las relaciones telemáticas será un hito. Créame: conozco a compañías británicas que llevan años intentando llevar a cabo proyectos de identificación global, y todavía no han conseguido poner de acuerdo a sus clientes para aunar todos los identificadores en curso en ese país y transformarlos en uno solo. En España este problema está culturalmente superado.

A efectos técnicos, y hasta donde sabemos, la DGP tiene las ideas muy claras y muy avanzadas.

– ¿Han previsto el uso del futuro DNI en los sistemas de la Seguridad Social?

– En nuestra arquitectura de seguridad en la que interviene la PKI, estamos preparados para tratarnos con otras autoridades de certificación; actualmente, y como es sabido, reconocemos a la FNMT-RCM, y en su momento estaremos listos para hacer lo propio con la DGP.

– Pregunta obligada: ¿está contento con el presupuesto de que dispone específicamente para seguridad?

– Los presupuestos para inversiones que hemos presentado para el Ejercicio de 2004, que no son bajos precisamente, nos los han aprobado. En este sentido tengo que manifestar que contamos con el apoyo decidido de nuestra Subdirección General.

– ¿Tiene idea de cuánto necesitaría crecer en personal el Centro de Calidad, Auditoría y Seguridad para afrontar los proyectos iniciados, los que están esperando arrancar y los que están en fases previas?

– Que vamos a incrementar nuestro personal experto en seguridad TIC, en calidad y en auditoría es algo que tengo claro; lo que no me atrevo es a avanzar cifras concretas. ■

Texto: **José de la Peña Muñoz**
Fotografía: **Jesús A. de Lucas**