# La seguridad de la información en la Administración presupuestaria

**El rol de Responsable de Seguridad de la Información de la Secretaría de Estado de Presupuestos y Gastos y de la Intervención General de la Administración del Estado, ámbito funcional al que se hace referencia como Administración presupuestaria, tuvo su primer reflejo normativo a través de la Resolución de la Secretaria de Estado de Presupuestos y Gastos, de 8 de julio de 2002, para el control de accesos a las bases de datos de la Secretaría de Estado.**
**Posteriormente, mediante la Resolución de la Secretaría de Estado de Hacienda y Presupuestos, de 24 de mayo de 2005, se adaptó la terminología a la utilizada por la Normativa en materia de Protección de Datos para, entre otros avances, evitar confusiones entre los roles definidos en la normativa de protección de datos y en la Resolución de 2002.**

**MARÍA JESÚS CASADO ROBLEDO**
Responsable de Seguridad de la Información en el ámbito de la Secretaría de Estado de Presupuestos y Gastos y de la Intervención General de la Administración del Estado.

Con la Resolución de 27 de febrero de 2009, de la Secretaría de Estado de Hacienda y Prepuestos, se evolucionó a una política global de seguridad de los sistemas de información de la Administración Presupuestaria.

La Resolución vigente data de 21 de diciembre de 2015. Ha venido a suponer un cambio importante pues la política de seguridad, en el ámbito de la Administración presupuestaria, se ha adaptado al Esquema Nacional de Seguridad, a la línea 3 de la Estrategia de Seguridad Nacional y a la Estrategia de Ciberseguridad nacional y se ha alineado con la Política de Seguridad de la Información del Ministerio de Hacienda y Administraciones Públicas. Además, se regula la implicación de los responsables de los centros directivos de la Secretaría de Estado en la dirección del Comité de Coordinación de la Seguridad de la Información.

En el artículo séptimo de la Resolución se indica expresamente que el Responsable de Seguridad de la Información asume las funciones de ese rol en los términos establecidos por la Ley Orgánica 15/1999, de protección de datos de carácter personal, el Esquema Nacional de Seguridad y la Política de Seguridad de la Información del Ministerio de Hacienda y Administraciones Públicas.

Entre sus cometidos figuran: Formar parte del Comité de Seguridad de la Información con el rol de Secretario con voz y voto; aplicar las medidas de seguridad de acuerdo con las directrices establecidas por el Comité; diseñar, construir, implantar y mantener las políticas, directrices, normativa, procedimientos, guías, instrucciones y herramientas relacionadas con la Seguridad de la Información y,

| Resolución 21 diciembre 2015 | RD 1720/2007 | RD 3/2010, Guías CCN-STIC 801 y 802 | Orden HAP/1953/2014 |
|---|---|---|---|
| Comité de Coordinación de la Seguridad de la Información | - | Comité de la Seguridad de la Información | |
| El Interventor General de la Administración del Estado y los directores generales de los centros directivos de la Secretaría de Estado de Presupuestos y Gastos, que actuarán rotatoriamente, cada seis meses, como presidente del Comité. | | | |
| Coordinador de los SIP que actuará como Vicepresidente del Comité, y Subdirecciones IP | - | Responsable del sistema | Responsable del sistema |
| Responsable de Seguridad de la Información | Responsable de seguridad | Responsable de seguridad. | Responsable de seguridad |
| Responsable de centro/Responsable de fichero | Responsable del fichero | Responsable de la información | Responsable de la información |
| Responsable de centro/Responsable de fichero | - | Responsable del servicio | Responsable del servicio |
| Subdirecciones Generales de Aplicaciones de Contabilidad y Control, Presupuestos y Fondos Comunitarios, Costes de Personal Activo y Pasivo, Subdirección General de Explotación. Subdirectores, Adjuntos, Jefes de Área y Jefes de Proyecto de dichas Subdirecciones | - | Administrador de seguridad del sistema | |
| Usuarios | - | - | |

**TABLA 1: Disposiciones relativas al Comité de Coordinación de la Seguridad en la información**

bajo la iniciativa y coordinación del Responsable de Seguridad de la Información en los servicios de Informática presupuestaria, se administrará la seguridad de los sistemas.

### Retos de futuro

La adaptación al Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE, que ha entrado en vigor el 24 de mayo y se aplicará a partir del 25 de mayo de 201, requerirá de un trabajo importante para alcanzar los objetivos marcados.

De la misma forma, en el ejercicio del rol de DPO (en la actualidad mi cargo es el de Responsable de Seguridad en los términos regulados) se tendrán que abordar funciones y asumir responsabilidades propias del cargo, entre otras normas, por la Ley Orgánica de Protección de Datos.

Asimismo, la a adaptación a los cambios introducidos en el Esquema Nacional de Seguridad por el Real Decreto 951/2015 y la evolución del comportamiento de "los malos" que se conocen a través de los informes emitidos por el Centro Criptológico Nacional y de los avisos que se reciben del Instituto Nacional de Ciberseguridad (INCIBE) suponen retos importantes que requerirán nuestro esfuerzo.

Los informes del CCN nos permiten proponer acciones estructurales y los avisos de INCIBE facilitan la concienciación de los usuarios y la configuración las medidas de seguridad coyunturales en los sistemas por los que pueden entrar los posibles incidentes: por ejemplo, en el correo

electrónico. Si bien, los avisos de INCIBE, están más orientados a las personas por lo que permiten enviar correos informativos advirtiendo de los efectos adversos. Son útiles porque no sólo sirven para preservar a la Administración presupuestaria, sino que resultan de aplicación directa en sus ordenadores personales y en su comportamiento dentro de su vida privada. Cabe destacar la encomiable labor de ambas instituciones, cada una en el ámbito de sus competencias.

## Gobernanza de la seguridad

En relación con la creencia de que la figura del CISO bloquea las iniciativas del CIO, se ha de puntualizar que no es el caso de la Administración presupuestaria. En base a la primera Resolución que se aprobó en 2002 y que fue iniciativa del CIO, las siguientes Resoluciones que han recogido la evolución natural de la necesidad de la seguridad han sido apoyadas por el CIO y aprobadas colegiadamente en el Comité de Seguridad de la Información que empezó su trabajo en 2002.

A su vez el CIO recibió muy positivamente la propuesta de que la estructura del Comité se adaptase a la estructura del Consejo de Seguridad Nacional incluyendo la figura de Presidente del Comité asignado a los máximos responsables de las Unidades que conforman la Administración presupuestaria: Interventor General de la Administración del Estado, Director General de Presupuestos, Director General de Costes de Personal y Pensiones Públicas y Director General de Fondos Comunitarios. Cada uno de ellos ejerce de presidente de forma rotatoria cada seis meses.

Esta estructura está regulada en la Resolución que está en vigor y ya se ha celebrado la primera reunión presidida por el Interventor General. Su participación ha sido muy positiva pues lo primero que solicitó fue un estudio sobre la proporcionalidad entre la funcionalidad y la seguridad. El resultado ha sido muy favorable para la seguridad de la información ya que ha entendido que es facilitadora y no un lastre.

La segregación de funciones es una máxima en la Administración presupuestaria. En la Resolución vigente se recoge el nivel de segregación de funciones alcanzado, siguiendo otra máxima tan importante como la anterior: estudiar muy detenidamente la necesidad de crear roles distintos a los existentes con el objeto de evitar conflictos de intereses.

En la Administración presupuestaria se ha alcanzado un hito más que significativo al incluir la función de seguridad de la información en el RD vigente por el que se desarrolla la estructura orgánica básica del Ministerio de Hacienda y Administraciones Públicas mediante el Real Decreto 802/2014, de 19 de septiembre.

Actualmente el CISO depende del CIO, ahora bien, puede ser transitorio, no obstante, el proceso no está lo suficientemente maduro para plantearse a corto plazo esta segregación. Se ha de considerar que la Administración presupuestaria está en la senda correcta, se está avanzando sin prisa, pero sin pausa.

## Medidas concretas

Basándose en la experiencia adquirida desde enero de 2003 hasta la fecha, bien se puede considerar que es necesario:

- Evitar asimilar la Seguridad de la Información con la Seguridad Informática.
- Que el conocimiento sobre Seguridad de la Información resida en la Organización. Contar con la colaboración estrecha con la industria para aprovechar su conocimiento de la evolución tecnológica y de las tendencias para resolver las necesidades de protección de la información.
- Dotar de medios, sobre todo de personas, disponer de una estructura.
- Tener presente el principio de proporcionalidad para garantizar el equilibrio entre funcionalidad y seguridad.
- Un CISO ha de conocer la misión del Departamento en el que ejerce su función. En las Administraciones Públicas es fácil pues se regula en los Reales Decretos mediante los que se desarrollan las estructuras básicas de los Departamentos Ministeriales. No obstante, este conocimiento es de alto nivel por tanto es necesario descender y conocer la normativa de desarrollo, entre otras la normativa que regulan los procedimientos administrativos que permiten cumplir con la misión.
- Ha de estar capacitado para comprender los requerimientos de los responsables de la gestión, transmitirles que la seguridad es facilitadora y no un impedimento. Para ello el CISO ha de ser un buen comunicador.
- Esa misma capacidad ha de tenerla con los responsables de la tecnología.

Ello permitirá que sirva de nexo de unión entre ambos colectivos consiguiendo que las medidas de seguridad técnicas estén alineadas con las medidas organizativas y normativas.

Todo ello es esencial para poder transponer la normativa de Seguridad de la Información al Departamento en el que ejerce su función y que las medidas que se adopten ya sean organizativas, normativas o técnicas se puedan aplicar. ✱