

Fundación SOCINFO

Seguridad IT (10): Informe del estado de la seguridad, Auditoría y certificación de conformidad

Madrid, 30 de marzo de 2016

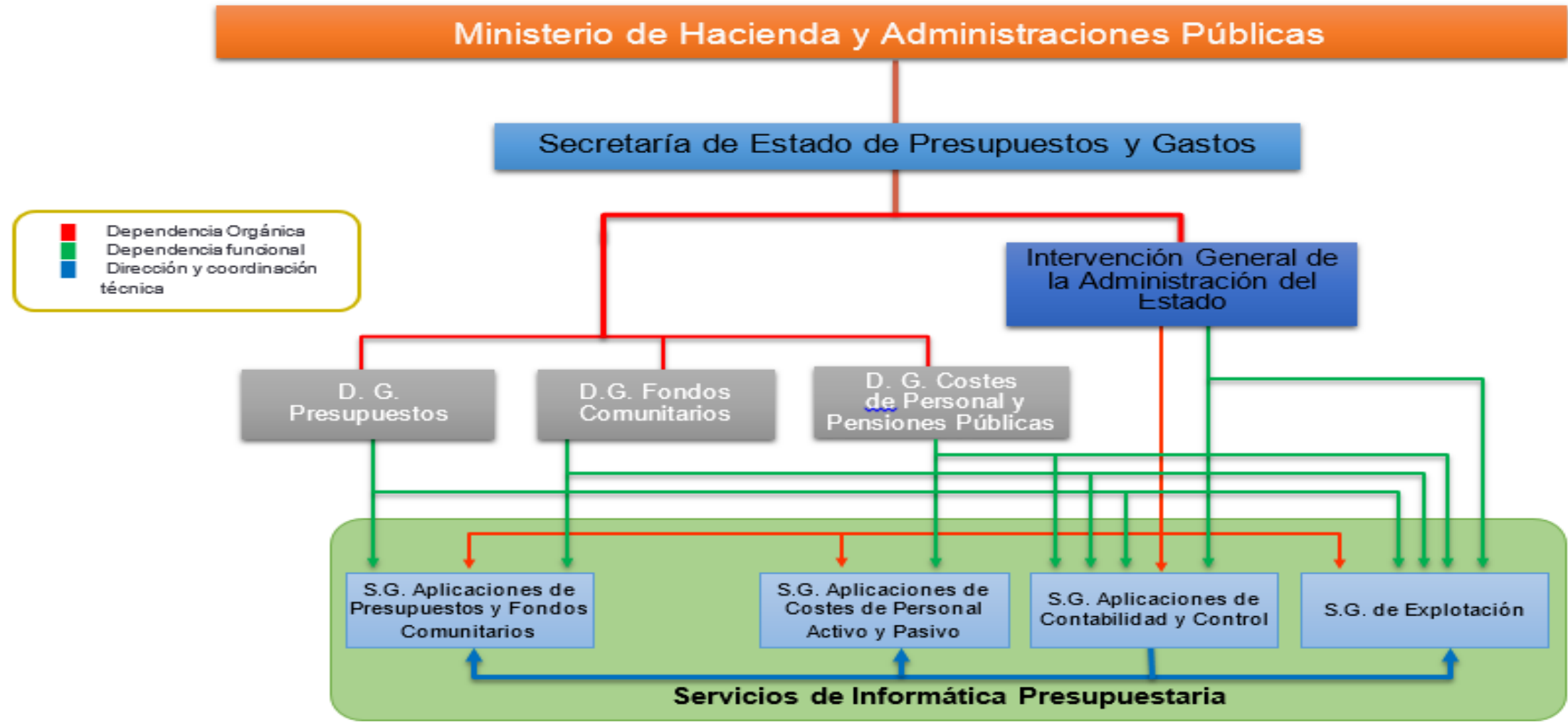
María Jesús Casado Robledo

Responsable de Seguridad de la Información

Secretaría de Estado de Presupuestos y Gastos

Intervención General de la Administración del Estado

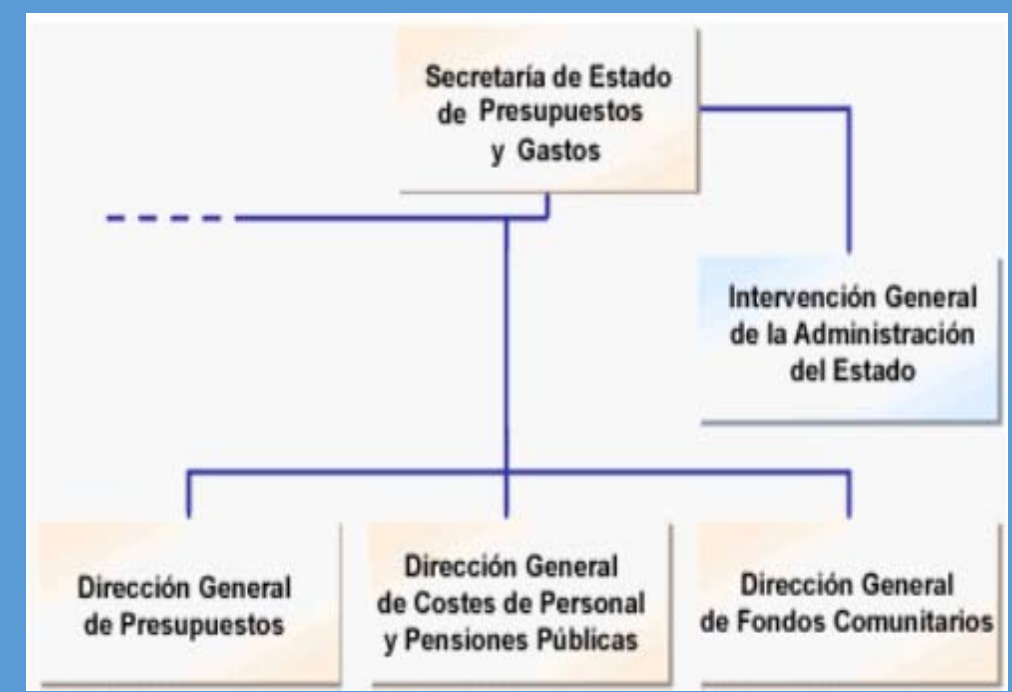
1. Secretaría de Estado de Presupuestos y Gastos e Intervención General de la Administración del Estado
2. Informe del estado de la seguridad
3. Auditoría y certificación de conformidad con el ENS



Secretaría de Estado de Presupuestos y Gastos

Dirigir y coordinar

- Planificación, programación y presupuestación del sector público estatal y de sus costes de personal.
- Diseño, planificación y gestión de los fondos destinados a la política económica regional.
- Seguimiento y gestión de la participación española en el presupuesto de la Unión Europea



Intervención General de la Administración del Estado

- Control interno de la gestión económico-presupuestaria.
- Seguimiento y control de subvenciones y ayudas públicas.
- Autoridad de auditoria de programas comunitarios en los que la IGAE coordina las acciones de protección de los intereses de la UE.
- Relación con las haciendas territoriales a efectos de la información contable que deben remitir para la formación de las cuentas económicas del sector público.
- Integración, gestión y publicación del inventario de Entres del Sector Público Estatal, Autonómico y Local.
- Asesoramiento a los órganos de gestión en sus funciones de control, gestión de la información económico-financiera relacionada con el ejercicio de sus funciones contables y de control.
- Auxilio y colaboración con la Administración de Justicia.
- Planificación, diseño y ejecución de la política informática de la Administración presupuestaria.
- Soporte informático de las actividades y el asesoramiento, coordinación e instrumentación de los proyectos informáticos de sus órganos y la seguridad de la información.



1. Informe del estado de la seguridad

Evaluación periódica del estado de la seguridad de los sistemas (artículo 35 RD 3/2010)

Pestaña 3/10. Apartado 2 “nivel de implantación del proceso de seguridad” en relación con el desarrollo normativo y su cumplimiento

- Número total de normas de seguridad previstas.
- Número de normas de seguridad implantadas. Indicar, en cifras, el número total de normas de seguridad que el organismo ha aprobado y **difundido**.

Septiembre de 2011. Mejora continua. Justificación: el proceso de elaboración, revisión, actualización, aprobación y aplicación comenzó en julio de 2002.

Evaluación periódica del estado de la seguridad de los sistemas (artículo 35 RD 3/2010)

Pestaña 4/10. Elementos del ENS

- Gestión de cambios (OP.EXP.4, OP.EXP.5)
 - Atendiendo a la seguridad: instalación inmediata.
 - Atendiendo a la funcionalidad: verificación de compatibilidad

Evaluación periódica del estado de la seguridad de los sistemas (artículo 35 RD 3/2010)

Pestaña 8/10. Auditorías

- Auditorías del ENS.
- Auditorías técnicas.
- Certificaciones de seguridad.

Número de deficiencias de impacto ALTO detectadas.

Número de deficiencias de impacto MEDIO detectadas.

Evaluación periódica del estado de la seguridad de los sistemas (artículo 35 RD 3/2010)

Pestaña 10/10. Medidas de seguridad

Cumplimiento	Explicación orientativa
10%	La medida de seguridad se cumple de forma muy parcial, casi anecdótica.
50%	La medida de seguridad se cumple en gran medida, pero no en toda su amplitud o no en todos los sistemas de información.
90%	La medida de seguridad se cumple de manera generalizada.
95%	La medida de seguridad no sólo se cumple de manera generalizada sino que sus excepciones han sido contempladas.

Evaluación periódica del estado de la seguridad de los sistemas (artículo 35 RD 3/2010)

INES

- Porcentajes.
- Números absolutos.
 - Normas a desarrollar, implantadas.
 - Días para instalar parches.

Auditoría

- Trabajo independiente.
- Visión más cercana a la realidad.
 - De las normas implantadas cuantas son conocidas por los usuarios. Además de conocerlas cuantos usuarios las aplican.

2. Auditoría y certificación de conformidad con el ENS

Seguridad IT (VIII): Esquema Nacional de Seguridad. Plan Nacional de Ciberseguridad

11 de febrero de 2014

- *Esperar las auditorías.* Sin miedo sino como mejoras

Auditoría de cumplimiento del ENS en el ámbito de la Administración presupuestaria

- 22 de enero de 2016.
- Equipo de Auditoría Informática de la S.G. de Aplicaciones de Contabilidad y Control de la IGAE.

Auditoría de cumplimiento del ENS en el ámbito de la Administración presupuestaria

Ha llegado la hora de la verdad

- Normas
 - Proceso formal de revisión.
 - Divulgación. Siempre es insuficiente.
- Personas
 - ¿Cómo hacemos?.
- Tecnología

Lo de siempre: recursos

Certificación de conformidad



A la espera

- Instrucción técnica de seguridad que regule el procedimiento de acreditación de las entidades que puedan emitir certificaciones de conformidad.

Supondrá

- Transmitir confianza.
- Reconocimiento a la labor realizada.

Gracias por su atención