Hoja de ruta para el cumplimiento del esquema nacional de seguridad por las administraciones locales.
Cuaderno de Recomendaciones

ENS:

MARCO LEGAL , PRINCIPALES ROLES, DIAGRAMA GENERAL – FASES PRINCIPALES, CONFORMIDAD CON EL ENS

Prof. Dr. Carlos Galán
cgalan@atl.es

9 de octubre de 2017

El Esquema Nacional de Seguridad (ENS): Marco Legal, Roles y Funciones, Diagrama General y Conformidad

Semblanza del ponente

Carlos Galán es Doctor en Informática, Abogado especialista en Derecho de las Tecnologías de la Información, *Certified Information Security Manager* (CISM) por ISACA, Consultor/Formador Homologado de la EOI y Auditor Técnico de la Entidad Nacional de Acreditación (ENAC) para el ENS y el Reglamento Europeo eIDAS.

Autor de una decena de libros relacionados con las Tecnologías de la Información, su Derecho y sus aplicaciones, ha escrito asimismo una multiplicidad de artículos y comentarios en prensa y publicaciones especializadas. Ha desarrollado parte de su carrera profesional en el Grupo Telefónica, ocupando diversos cargos y participando en importantes proyectos nacionales e internacionales.

Ha sido Vocal Asesor y Director de la Oficina de Modernización del Ministerio del Interior, donde, entre otras actividades, diseñó en Plan de Modernización de los Cuerpos y Fuerzas de Seguridad del Estado y presidido la Comisión de Informática y Comunicaciones de la Seguridad de los Juegos Olímpicos de Barcelona ’92.

Ha sido profesor de la Facultad de Informática de la Universidad Politécnica de Madrid, de la Escuela Técnica Superior de Ingenieros Industriales de la UNED, de la licenciatura de Administración y Dirección de Empresas de la Universidad Complutense de Madrid y del Instituto de Postgrado de la Universidad Pontificia de Comillas.

Ha sido Director General de la Agencia de Certificación Electrónica ACE (primera Autoridad de Certificación de España), Vicepresidente de la Asociación de Entidades de Confianza Digital AECODI, Director General de Desarrollo y Tecnología de la Fundación General de la Universidad de Málaga y Presidente del Comité de Nuevas Tecnologías de Hispajuris, la mayor red de despachos de abogados de España.

En el terreno académico, ha sido profesor de *Calidad, Seguridad y Protección de la Información*, de la Ingeniería de Informática de la Universidad Pontificia de Salamanca. Actualmente es miembro del Área de Derecho Administrativo de la Universidad Carlos III de Madrid, institución en la que imparte *Derecho de las TIC* en el Grado de Derecho de la Facultad de Ciencias Sociales y Jurídicas, y *Aspectos Legales de la Ingeniería Informática,* en el Máster de *Derecho de las Telecomunicaciones y Tecnologías de la Información,* actividades que compagina con la escritura de monografías y artículos y el dictado de conferencias y cursos donde es ponente habitual en las materias relativas al Derecho de las Tecnologías de la Información y las Comunicaciones, la Administración Electrónica, Firma Electrónica, Certificación Digital y Seguridad IT.

Ha sido asesor parlamentario en la redacción de la Ley 59/2003, de firma electrónica y, en la actualidad, es colaborador del Ministerio de Hacienda y Administraciones Públicas -dónde es miembro del Grupo de Expertos del Plan de Acción de Administración Electrónica 213-2015- y del Centro Criptológico Nacional –del Centro Nacional de Inteligencia-, en Administración Electrónica y Ciberseguridad, colaborando asimismo con varias organizaciones públicas y privadas. Es Presidente de la Agencia de Tecnología Legal, vicepresidente de la Comisión de Contratación Electrónica de la Asociación Nacional de Empresas de Internet, miembro del Observatorio Notarial para la Sociedad de la Información y miembro del Observatorio de la Mesa de la Justicia del Ilustre Colegio de Abogados de Madrid.

(← volver)

Parte I. Marco Legal

El origen: El Acceso Electrónico de los Ciudadanos a los Servicios Públicos (Ley 11/2007)

Y la confirmación: Ley 39/2015, Procedimiento Administrativo Común de las AA.PP.
Ley 40/2015, Régimen Jurídico del Sector Público

Artículo 42. Esquema Nacional de Interoperabilidad y Esquema Nacional de Seguridad.

Ley 11/2007

1. El **Esquema Nacional de Interoperabilidad** comprenderá el conjunto de criterios y recomendaciones en materia de seguridad, conservación y normalización de la información, de los formatos y de las aplicaciones que deberán ser tenidos en cuenta por las Administraciones Públicas para la toma de decisiones tecnológicas que garanticen la **interoperabilidad**.

2. El **Esquema Nacional de Seguridad** tiene por objeto 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**.

Ley 40/2015

Artículo 156. Esquema Nacional de Interoperabilidad y Esquema Nacional de Seguridad.

1. El **Esquema Nacional de Interoperabilidad** comprenderá el conjunto de criterios y recomendaciones en materia de seguridad, conservación y normalización de la información, de los formatos y de las aplicaciones que deberán ser tenidos en cuenta por las Administraciones Públicas para la toma de decisiones tecnológicas que garanticen la **interoperabilidad**.

2. El **Esquema Nacional de Seguridad** tiene por objeto 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 garanticen adecuadamente la **seguridad de la información tratada.**

Ley 39/2015 – Procedimiento Administrativo Común de las AA.PP.

Art. 13. Derechos de las personas en sus relaciones con las Administraciones Públicas

h) A la protección de datos de carácter personal, y en particular a la **seguridad** y **confidencialidad** de los datos que figuren en los ficheros, sistemas y aplicaciones de las Administraciones Públicas.

Art. 16. Registro

1... Tanto el Registro Electrónico General de cada Administración como los registros electrónicos de cada Organismo cumplirán con las garantías y medidas de seguridad previstas en la legislación en materia de protección de datos de carácter personal.

centro nacional de inteligencia
centro criptológico nacional

Agencia de Tecnología Legal

Art. 17. Archivo de documentos

3. Los medios o soportes en que se almacenen documentos, deberán contar con medidas de seguridad, de acuerdo con lo previsto en el ENS que garanticen la integridad, autenticidad, confidencialidad, calidad, protección y conservación de los documentos almacenados. En particular, asegurarán la identificación de los usuarios y el control de accesos, así como el cumplimiento de las garantías previstas en la legislación de protección de datos.

Art. 27. Validez y eficacia de las copias realizadas por las Administraciones Públicas

Las copias auténticas tendrán la misma validez y eficacia que los documentos originales.

3. Para garantizar la identidad y contenido de las copias electrónicas o en papel, y por tanto su carácter de copias auténticas, las Administraciones Públicas deberán ajustarse a lo previsto en el Esquema Nacional de Interoperabilidad, el ENS y sus normas técnicas de desarrollo.

Art. 28. Documentos aportados por los interesados al procedimiento administrativo.

3... Se presumirá que esta consulta es autorizada por los interesados, salvo que conste en el procedimiento su oposición expresa o la ley especial aplicable requiera consentimiento expreso, debiendo, en ambos casos, ser informados previamente de sus derechos en materia de protección de datos de carácter personal.

Art. 31 Cómputo de plazos en los registros

2. El registro electrónico de cada Administración u Organismo se regirá a efectos de cómputo de los plazos, por la fecha y hora oficial de la sede electrónica de acceso, que deberá contar con las medidas de **seguridad** necesarias para garantizar su integridad y figurar de modo accesible y visible

Art. 40. Notificación

5. Las Administraciones Públicas podrán adoptar las medidas que consideren necesarias para la **protección** de los datos personales que consten en las resoluciones y actos administrativos, cuando éstos tengan por destinatarios a más de un interesado.

Disposición adicional segunda. Adhesión de las Comunidades Autónomas y Entidades Locales a las plataformas y registros de la Administración General del Estado.

.. Opte por mantener su propio registro o plataforma, las citadas Administraciones deberán garantizar que éste cumple con los requisitos del Esquema Nacional de Interoperabilidad, el ENS, y sus normas técnicas de desarrollo.

Ley 40/2015
Art. 3. Principios generales

Artículo 3. *Principios generales.*

2. Las Administraciones Públicas se relacionarán entre sí y con sus órganos, organismos públicos y entidades vinculados o dependientes a través de medios electrónicos, que aseguren la interoperabilidad y seguridad de los sistemas y soluciones adoptadas por cada una de ellas, garantizarán la protección de los datos de carácter personal, y facilitarán preferentemente la prestación conjunta de servicios a los interesados.

Ley 40/2015 – Régimen Jurídico del Sector Público

Art. 38. Sede electrónica

2. El establecimiento de una sede electrónica conlleva la responsabilidad del titular respecto de la integridad, veracidad y actualización de la información y los servicios a los que pueda accederse a través de la misma.
Cada Administración Pública determinará las condiciones e instrumentos de creación de las sedes electrónicas, con sujeción a los principios de transparencia, publicidad, responsabilidad, calidad, **seguridad**, **disponibilidad**, accesibilidad, neutralidad e interoperabilidad.

Art. 44. Intercambio electrónico de datos en entornos cerrados de comunicación

4. En todo caso deberá garantizarse la **seguridad** del entorno cerrado de comunicaciones y la protección de los datos que se transmitan.

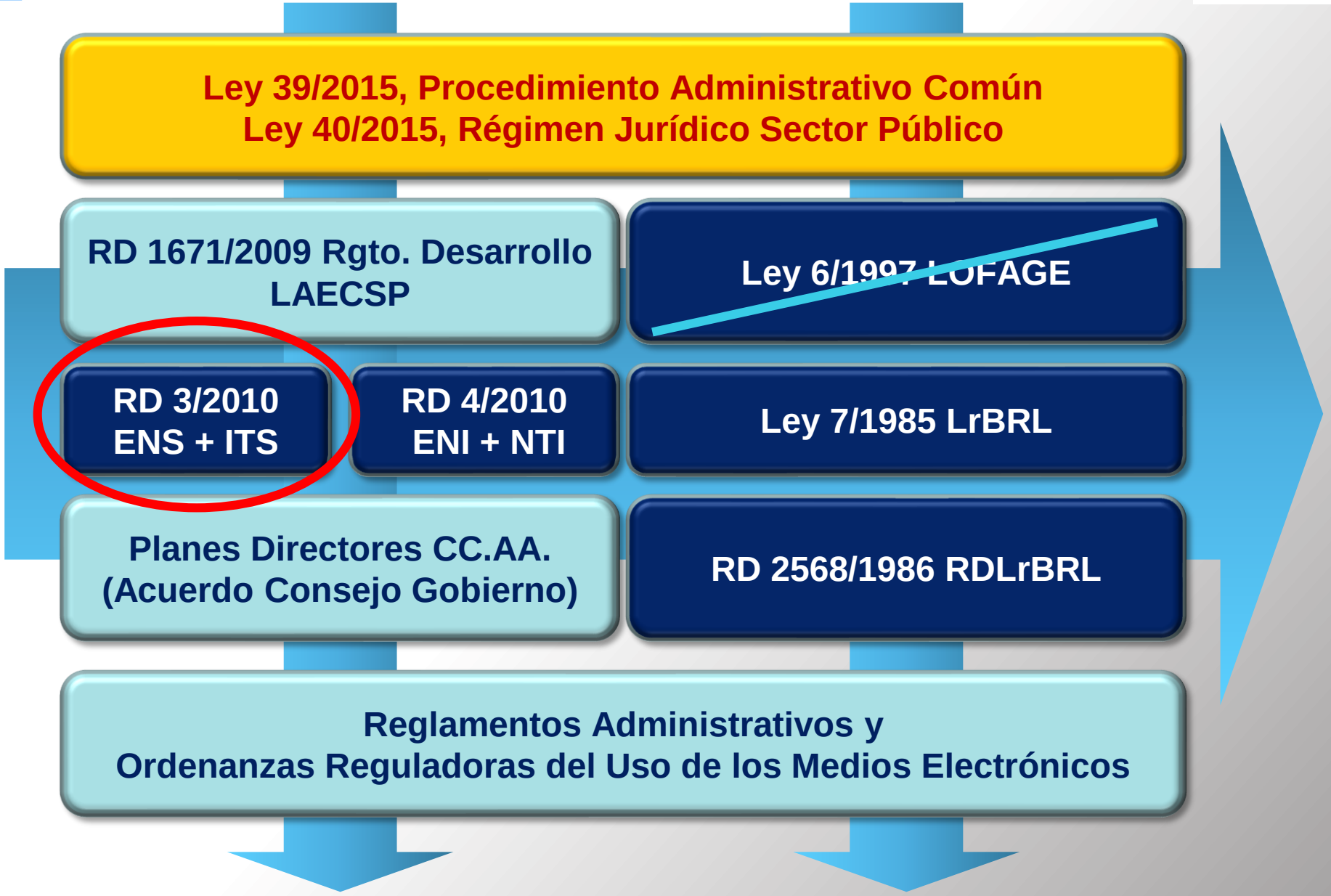
Art. 46. Archivo electrónico de documentos

3. Los medios o soportes en que se almacenen documentos, deberán contar con medidas de seguridad, de acuerdo con lo previsto en el ENS, que garanticen la integridad, autenticidad, confidencialidad, calidad, protección y conservación de los documentos almacenados. En particular, asegurarán la identificación de los usuarios y el control de accesos, el cumplimiento de las garantías previstas en la legislación de protección de datos, así como la recuperación y conservación a largo plazo de los documentos electrónicos producidos por las Administraciones Públicas que así lo requieran, de acuerdo con las especificaciones sobre el ciclo de vida de los servicios y sistemas utilizados

Art. 155. Transmisiones de datos entre Administraciones Públicas.

1. De conformidad con lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y su normativa de desarrollo, cada Administración deberá facilitar el acceso de las restantes Administraciones Públicas a los datos relativos a los interesados que obren en su poder, especificando las condiciones, protocolos y criterios funcionales o técnicos necesarios para acceder a dichos datos con las máximas garantías de **seguridad**, integridad y disponibilidad.

Marco jurídico actual



Instrucciones Técnicas de Seguridad

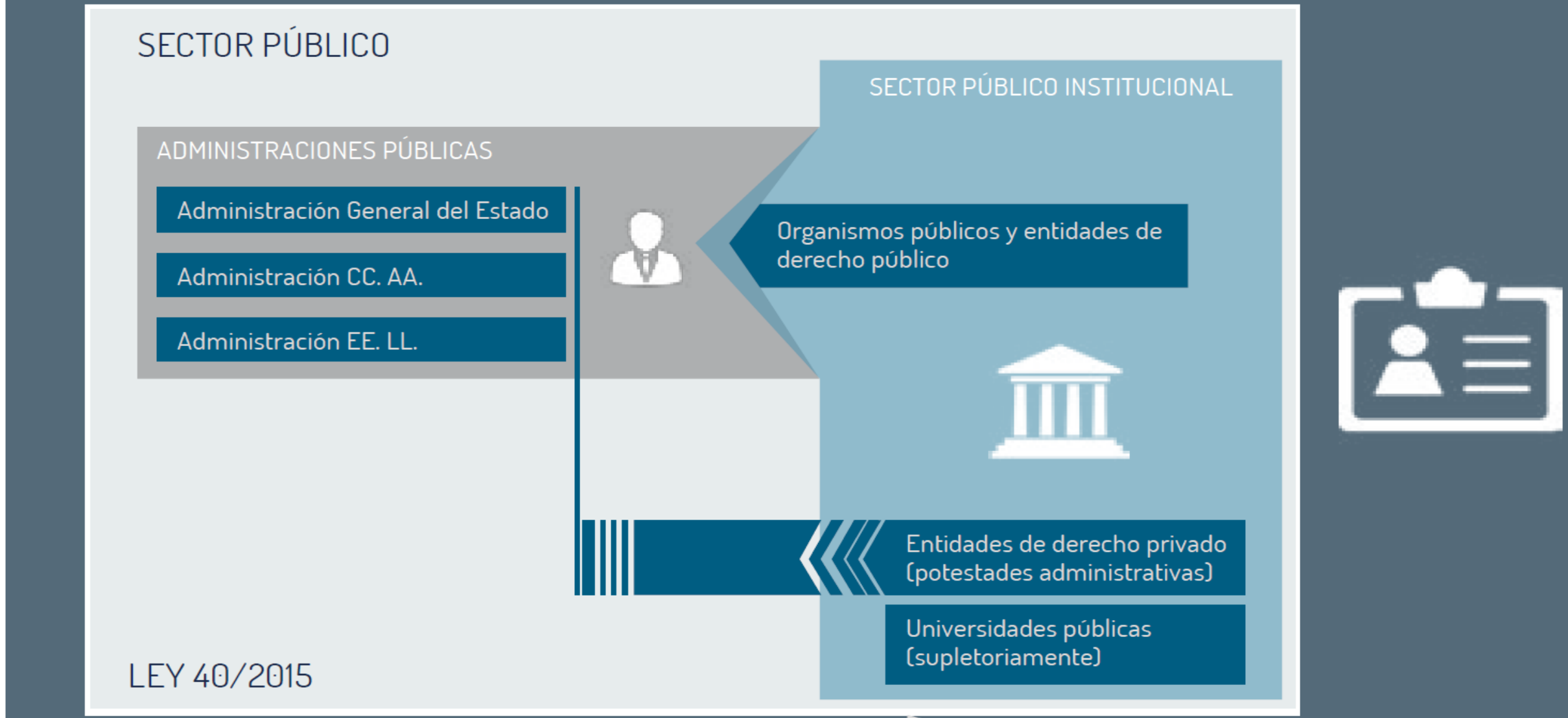
(29)

Ámbito de aplicación del ENS

De manera análoga a lo que sucede con buena parte del ordenamiento jurídico, el ámbito de aplicación del ENS es doble, a saber:

Por razón de los sujetos o entidades a los que se dirige la norma. → **ÁMBITO SUBJETIVO DE APLICACIÓN**

Por razón de las materias que son objeto de su regulación. → **ÁMBITO OBJETIVO o MATERIAL DE APLICACIÓN**



Ámbito subjetivo de aplicación del ENS

1. Sedes electrónicas.
2. Registros electrónicos.
3. Sistemas de Información accesibles electrónicamente por los ciudadanos, profesionales y empresas.
4. Sistemas de Información para el ejercicio de derechos (por parte de ciudadanos, profesionales y empresas).
5. Sistemas de Información para el cumplimiento de deberes (de los ciudadanos, profesionales y empresas; y de los organismos públicos, en su relación con los ciudadanos).
6. Sistemas de Información para recabar información y estado del procedimiento administrativo.
7. Sistemas de Información para el desarrollo del procedimiento administrativo.
8. Sistemas de Información para el cumplimiento de las misiones comprendidas en las competencias o potestades estatutarias del organismo en cuestión (todas aquellas que aparezcan en la norma de creación del organismo en cuestión y/o en sus estatutos, o para el cumplimiento de obligaciones legales.

ÁMBITO OBJETIVO o MATERIAL DE APLICACIÓN

- **Por tanto, en la medida que los sistemas de información del organismo en cuestión se utilicen -en todo o en parte- para la prestación de servicios o el desarrollo de las competencias o potestades estatutarias del organismo público en cuestión, resultará de aplicación lo dispuesto en el ENS.**

- **Y todos ellos, sea cual fuere la forma de prestación o ejecución de los servicios (propia, subcontratada, externa, concertada, modalidad Cloud Computing, en colaboración, etc.)**

- **Obsérvese que entre las medidas de seguridad previstas en el ENS (Anexo II) no están sólo aquellas relativas al acceso a los datos, sino también, y muy especialmente, aquellas relativas a su correcta custodia y conservación cuando tales datos se encuentran en forma electrónica.**

(← volver)

Parte II. Roles y Funciones

Mantenimiento y Gestión Seguridad IT

Requiere

Organización de Seguridad

Que identifique y defina:

1. **Actividades**,
2. **Responsabilidades**
3. **Estructura que las soporte**

En materia de Gestión de la Seguridad IT

ENS - Artículo 10. La seguridad como función diferenciada.

En los sistemas de información se diferenciará el responsable de la información, el responsable del servicio y el responsable de la seguridad.

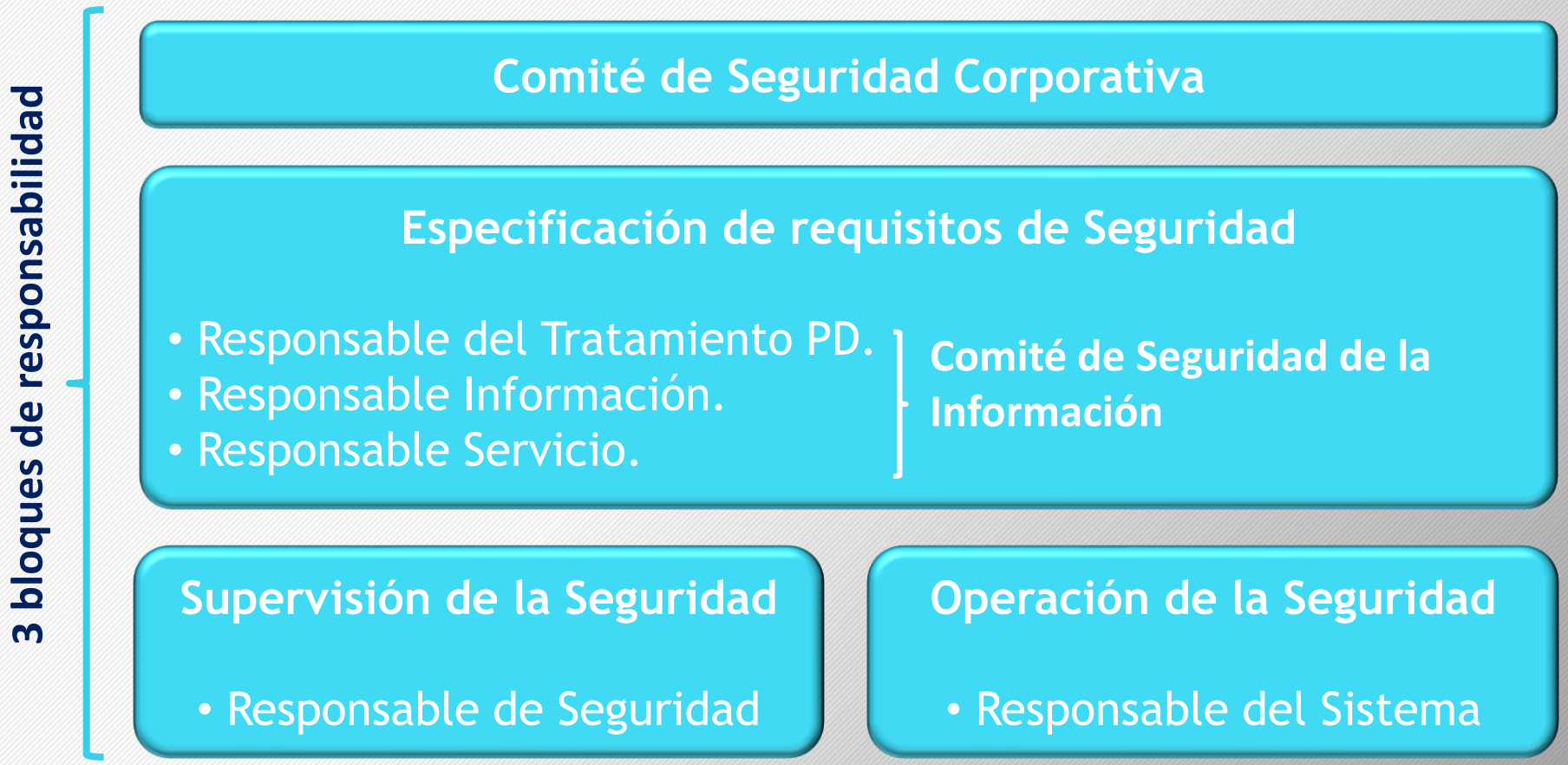
El **responsable de la información** determinará los requisitos de la información tratada; el **responsable del servicio** determinará los requisitos de los servicios prestados; y el **responsable de seguridad** determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios.

La responsabilidad de la seguridad de los sistemas de información estará diferenciada de la responsabilidad sobre la prestación de los servicios.

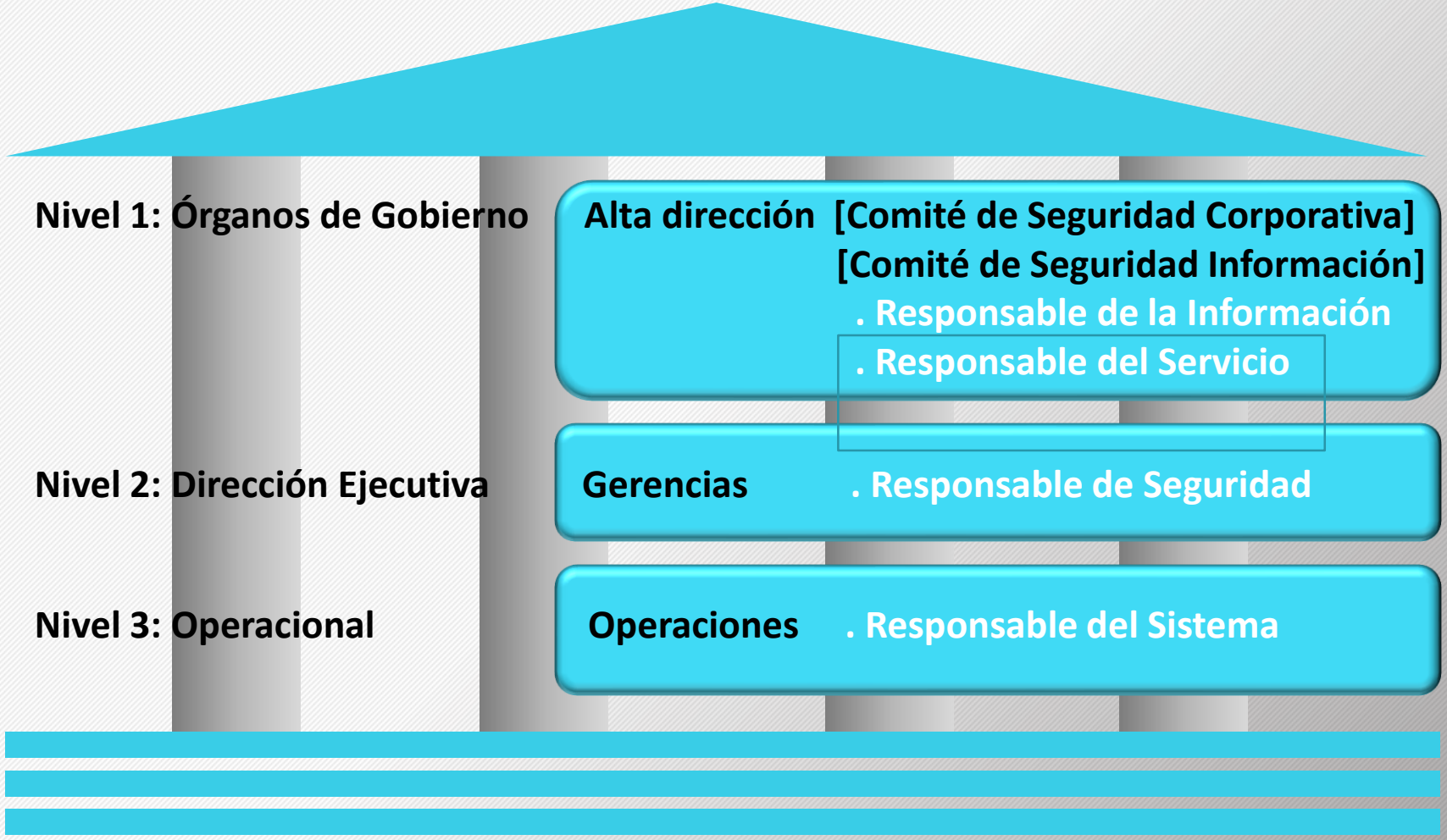
La **Política de Seguridad** de la organización detallará las atribuciones de cada responsable y los mecanismos de coordinación y resolución de conflictos.

ORGANIZACIÓN DE LA SEGURIDAD

Estructura Propuesta en la Guía CCN-STIC-801:



ORGANIZACIÓN DE LA SEGURIDAD



RESPONSABLES ESENCIALES

La **Dirección** del organismo es **responsable** de:

- Organizar las funciones y responsabilidades,
- la Política de Seguridad del organismo, y
- facilitar los recursos adecuados para alcanzar los objetivos propuestos.

Los directivos son también responsables de dar **buen ejemplo,** siguiendo las normas de seguridad establecidas.

En una organización pueden **coexistir diferentes informaciones y servicios**, debiendo identificarse al responsable (o propietario) de cada uno de ellos.

Una misma persona puede aunar varias responsabilidades.

RESPONSABLES ESENCIALES

RESPONSABLE DE LA INFORMACIÓN

(information owner)

- Ocupa un **alto cargo** en la dirección de la organización.
- Tiene la **responsabilidad última del uso** que se haga de la información y, por tanto, de su **protección**.
- Es el **responsable último de cualquier error o negligencia** que lleve a un incidente de confidencialidad o de integridad.
- El ENS asigna al 'Responsable de la Información' la potestad de establecer los **requisitos de la información en materia de seguridad** → determinar **los niveles de seguridad de la información.**

- Puede ser una **persona** o un **órgano corporativo**, que revestirá la forma de órgano colegiado de acuerdo con la normativa administrativa.

- Como se ha dicho, la aprobación formal de los niveles corresponde al Responsable de la Información, que puede recabar una propuesta al Responsable de la Seguridad y debe escuchar la opinión del Responsable del Sistema.

RESPONSABLES ESENCIALES

RESPONSABLE DEL SERVICIO

- Puede ser una **persona** o un **órgano corporativo** (que revestirá la forma de órgano colegiado de acuerdo con la normativa administrativa).
- Aunque la aprobación formal de los niveles corresponda al Responsable del Servicio, se puede recabar una propuesta al Responsable de la Seguridad y conviene que se escuche la opinión del Responsable del Sistema.

- La determinación de **los niveles de seguridad** en cada dimensión de seguridad debe realizarse dentro del marco establecido en el **Anexo I** del Esquema Nacional de Seguridad.
- Se recomienda **que los criterios de valoración estén respaldados por la Política de Seguridad** en la medida en que sean sistemáticos, sin perjuicio de que puedan darse criterios particulares en casos singulares.
- La prestación de un servicio siempre debe atender a los requisitos de seguridad de la información que maneja (a veces se dice que 'se heredan los requisitos'), y suele añadir requisitos de disponibilidad, así como otros como accesibilidad, interoperabilidad, etc.

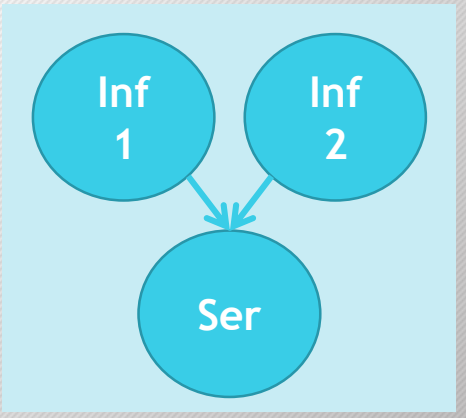
RESPONSABLES ESENCIALES

¿RESPONSABLE DE LA INFORMACIÓN = RESPONSABLE DEL SERVICIO?

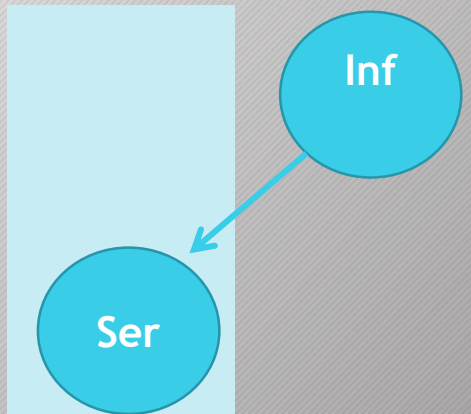
Es posible que coincidan en la misma persona u órgano las responsabilidades de la información y del servicio.

Sin embargo, la **diferenciación** tiene sentido:

- Cuando **el servicio maneja información de diferentes procedencias**, no necesariamente de la misma unidad departamental que la que presta el servicio.



- Cuando **la prestación del servicio no depende de la unidad que es Responsable de la Información**



RESPONSABLES ESENCIALES

RESPONSABLE DE LA SEGURIDAD

- Persona designada por la Dirección, según procedimiento descrito en su Política de Seguridad.

- **Responsabilidades**:

  - **Mantener la seguridad** de la información manejada y de los servicios prestados por los sistemas de información en su ámbito de responsabilidad, de acuerdo a lo establecido en la Política de Seguridad de la Organización.
  - **Promover la formación y concienciación** en materia de seguridad de la información dentro de su ámbito de responsabilidad.
  - Tareas del Anexo A de la Guía CCN-STIC-801.

RESPONSABLES ESENCIALES
DELEGACIÓN DE FUNCIONES

- Podrán designarse **Responsables de Seguridad Delegados** en caso de Sistemas de Información complejos, muy distribuidos o separados físicamente, o con muchos usuarios.
- La designación corresponde al Responsable de la Seguridad, a quién reportan.
- Se delegan funciones, no la responsabilidad.
- Los Delegados se harán cargo de todas aquellas acciones que delegue el Responsable de la Seguridad.
- Habitualmente → Seguridad de sistemas de información concretos o de sistemas de información horizontales.

RESPONSABLES OPERACIONALES

RESPONSABLE DEL SISTEMA

- Persona designada por la Dirección y figurará en la documentación de seguridad del sistema de información.

- Responsabilidades:
  - **Desarrollar, operar y mantener** el Sistema de Información durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.
  - **Definir la topología y sistema de gestión** del Sistema de Información estableciendo los criterios de uso y los servicios disponibles en el mismo.
  - **Cerciorarse de que las medidas específicas de seguridad se integren adecuadamente** dentro del marco general de seguridad.
  - El Responsable del Sistema puede acordar la suspensión del manejo de una cierta información o la prestación de un cierto servicio si es informado de deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos. **Esta decisión debe ser acordada con los Responsables de la Información afectada, del Servicio afectado y el Responsable de la Seguridad, antes de ser ejecutada**.
  - Las Tareas mencionadas en el Anexo A de la Guía CCN-STIC-801.

RESPONSABLES OPERACIONALES

ADMINISTRADOR DE LA SEGURIDAD DEL SISTEMA (ASS)

- Figurará en la documentación de seguridad del Sistema de información.
- Puede depender del Responsable del Sistema o del Responsable de la Seguridad.

- Funciones:

  - Implementación, gestión y mantenimiento de las medidas de seguridad.
  - Gestión, configuración y actualización, en su caso, del hw y sw en los que se base la seguridad.
  - Gestión de las autorizaciones concedidas a los usuarios del sistema.
  - Aplicación de los Procedimientos Operativos de Seguridad.
  - Aprobar los cambios en la configuración vigente del Sistema de Información.
  - Asegurar que los controles de seguridad establecidos son cumplidos estrictamente.
  - Asegurar que son aplicados los procedimientos aprobados para manejar el Sist. de Inf.
  - Supervisar las instalaciones de hardware y software, sus modificaciones y mejoras.
  - Monitorizar el estado de seguridad del sistema proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica.
  - Informar a los Responsables de la Seguridad y del Sistema de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad.
  - Colaborar en la investigación y resolución de incidentes de seguridad, desde su detección hasta su resolución.
  - Las restantes tareas, mencionadas en el Anexo A de la Guía CCN-STIC-801.

COMITÉS

- Algunas responsabilidades pueden instrumentarse por medio de Comités, que se articularán y funcionarán como órganos colegiados de acuerdo con la normativa administrativa.

- Son habituales los siguientes:

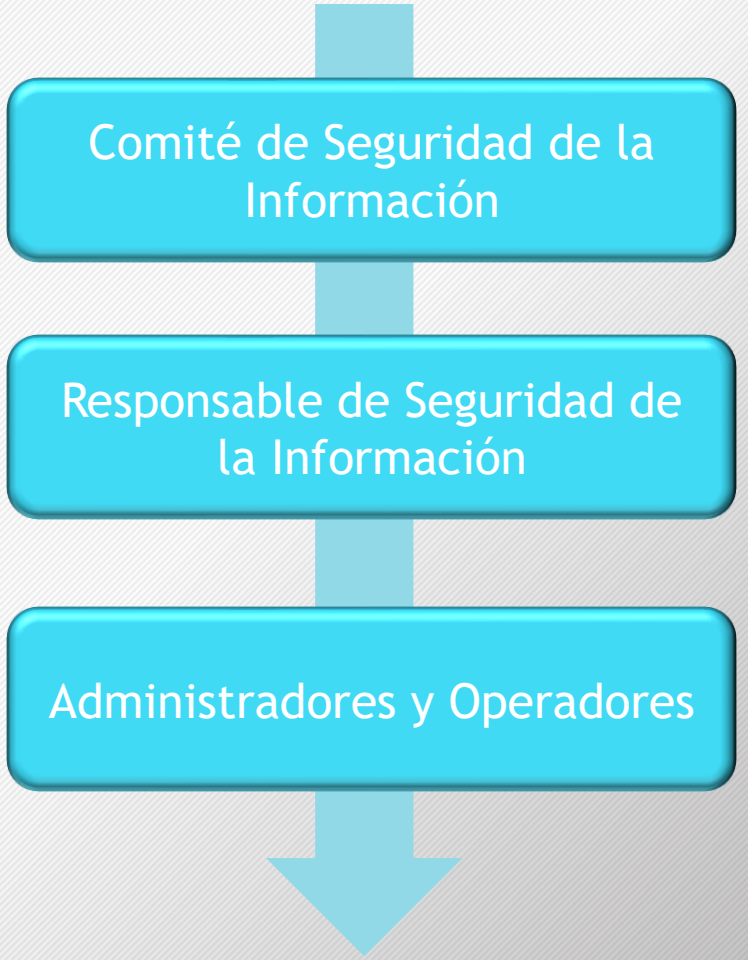
  - **Comité de Seguridad Corporativa**, que se responsabiliza de alinear todas las actividades de la organización en materia de seguridad: seguridad física, lógica y planes de contingencia.

  - **Comité de Seguridad de la Información**, que se responsabiliza de alinear las actividades de la organización en materia de seguridad de la información.

COMITÉS

COMITÉ DE SEGURIDAD DE LA INFORMACIÓN

Jerarquía Operativa



NOMBRAMIENTOS

- La Dirección del organismo nombra:
  - ✓ al **Responsable de la Información**; puede ser un cargo unipersonal o un órgano colegiado (típicamente, el Comité de Seguridad de la Información)
  - ✓ al **Responsable del Servicio**; puede ser el mismo que el Responsable de la Información; puede ser un cargo unipersonal o un órgano colegiado.
  - ✓ al **Responsable de la Seguridad**, que debe reportar directamente a la Dirección o, cuando existan, a los Comités de Seguridad de la Información y Seguridad Corporativa.
  - ✓ al **Responsable del Sistema**, que, en materia de seguridad, debe reportar al Responsable de la Seguridad

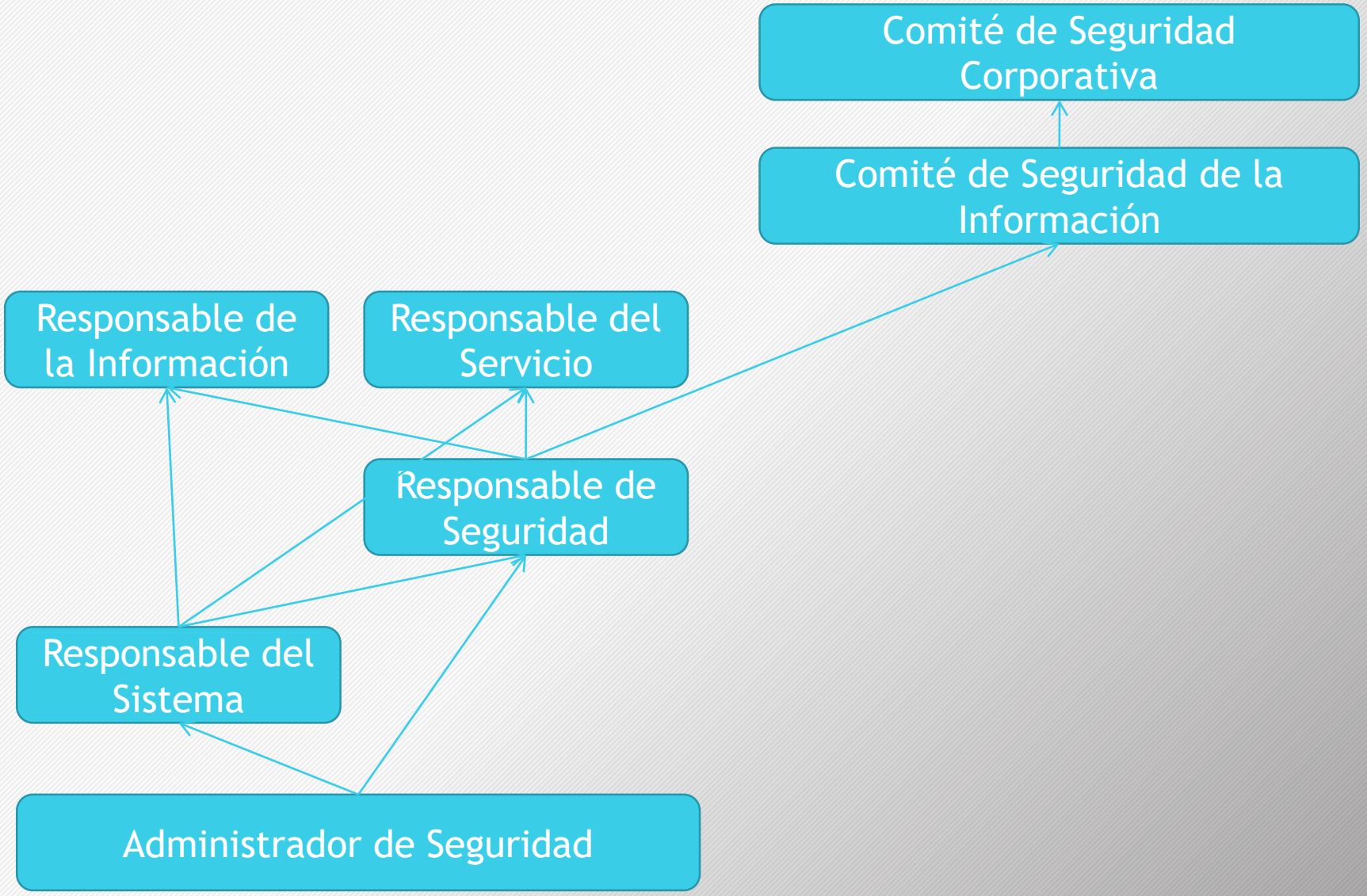
- El procedimiento de nombramiento de estos responsables debe constar en la Política de Seguridad de la Información de la Organización.

NOMBRAMIENTOS

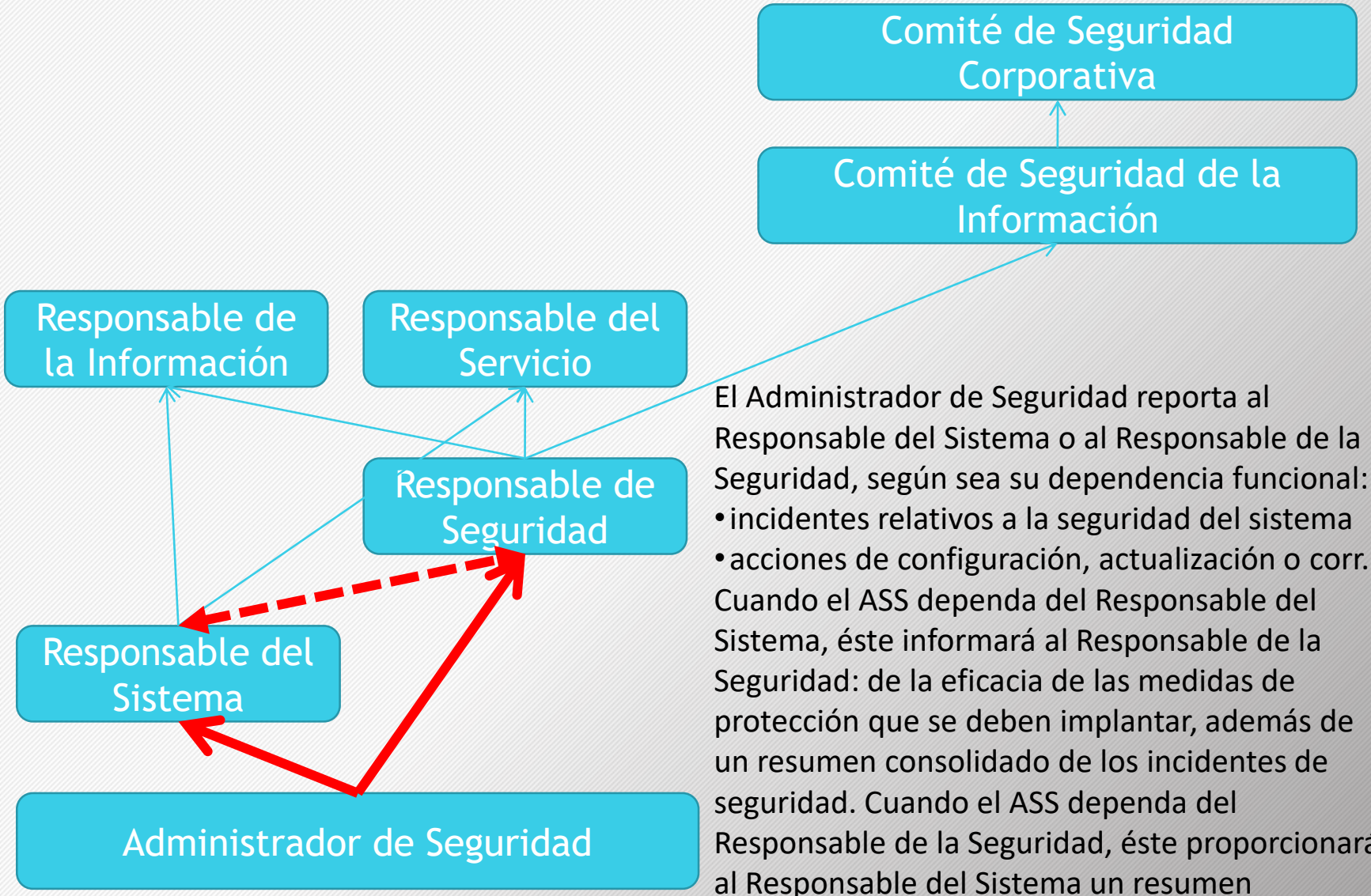
- La Dirección del organismo designará a la persona **Responsable del Sistema**:
  - ✓ a propuesta del Responsable de la Información tratada, cuando el Sistema de información trate una única información
  - ✓ a propuesta del Responsable del Servicio prestado, cuando el Sistema de información preste un único servicio.
  - ✓ directamente, cuando el Sistema de información trata diferentes informaciones o presta diferentes servicios, oídos los responsables de las informaciones y los servicios afectados.

- La Dirección del organismo designa al **Administrador de Seguridad del Sistema** a propuesta del responsable del mismo. Es muy recomendable que el nombramiento del Administrador de Seguridad sea formal y conste en la documentación de seguridad del sistema, reconociendo que sus funciones no son coyunturales, sino esenciales para cumplir las exigencias en materia de seguridad. No es nada recomendable que las funciones de esta persona se diluyan y sean realizadas por cualquier operador del sistema.

REPORTES


Comité de Seguridad Corporativa
Comité de Seguridad de la Información
Responsable de la Información
Responsable del Servicio
Responsable de Seguridad
Responsable del Sistema
Administrador de Seguridad

REPORTES

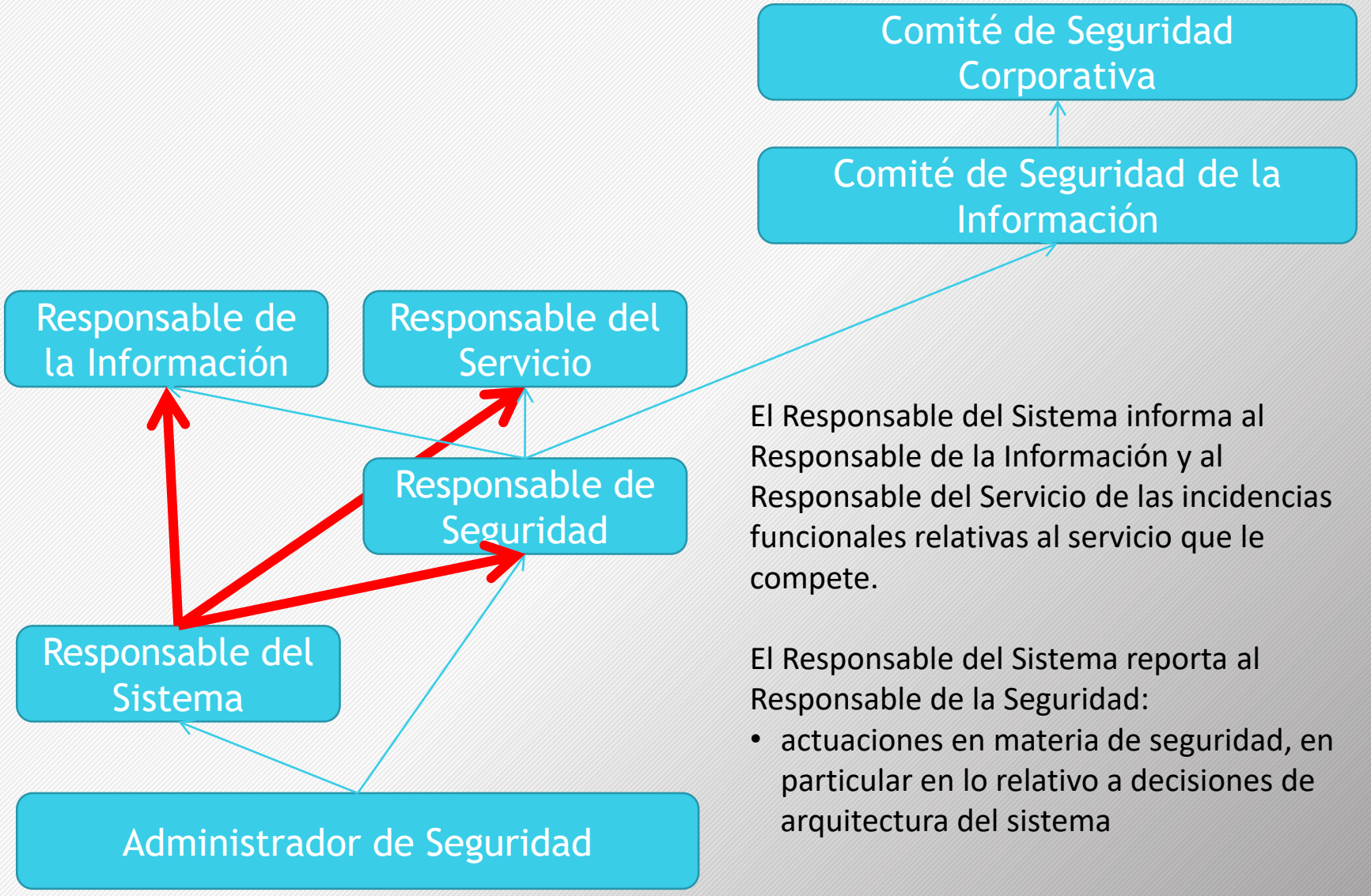


El Administrador de Seguridad reporta al Responsable del Sistema o al Responsable de la Seguridad, según sea su dependencia funcional:

- incidentes relativos a la seguridad del sistema
- acciones de configuración, actualización o corr.

Cuando el ASS dependa del Responsable del Sistema, éste informará al Responsable de la Seguridad: de la eficacia de las medidas de protección que se deben implantar, además de un resumen consolidado de los incidentes de seguridad. Cuando el ASS dependa del Responsable de la Seguridad, éste proporcionará al Responsable del Sistema un resumen consolidado de los incidentes de seguridad.

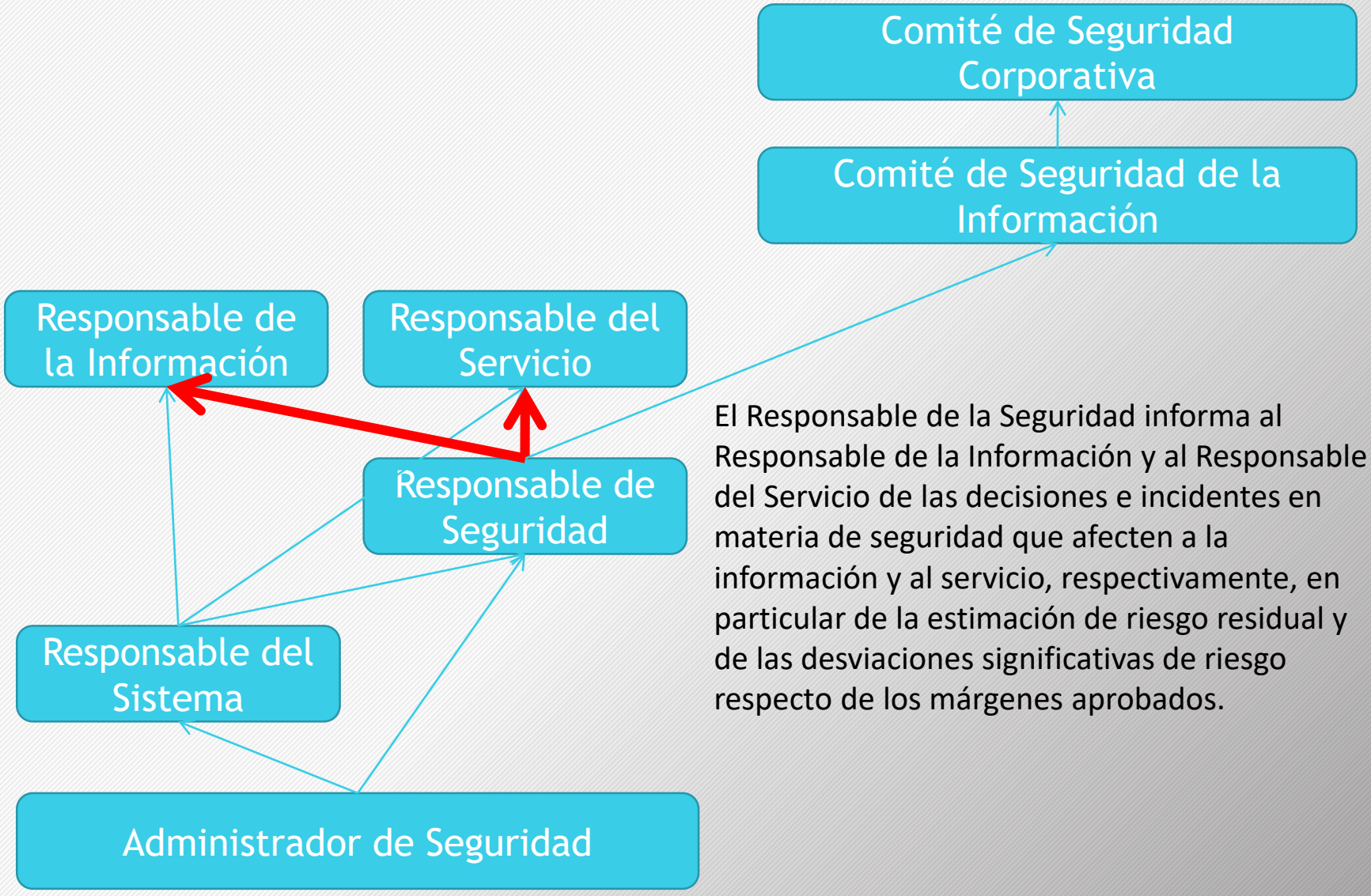
REPORTES



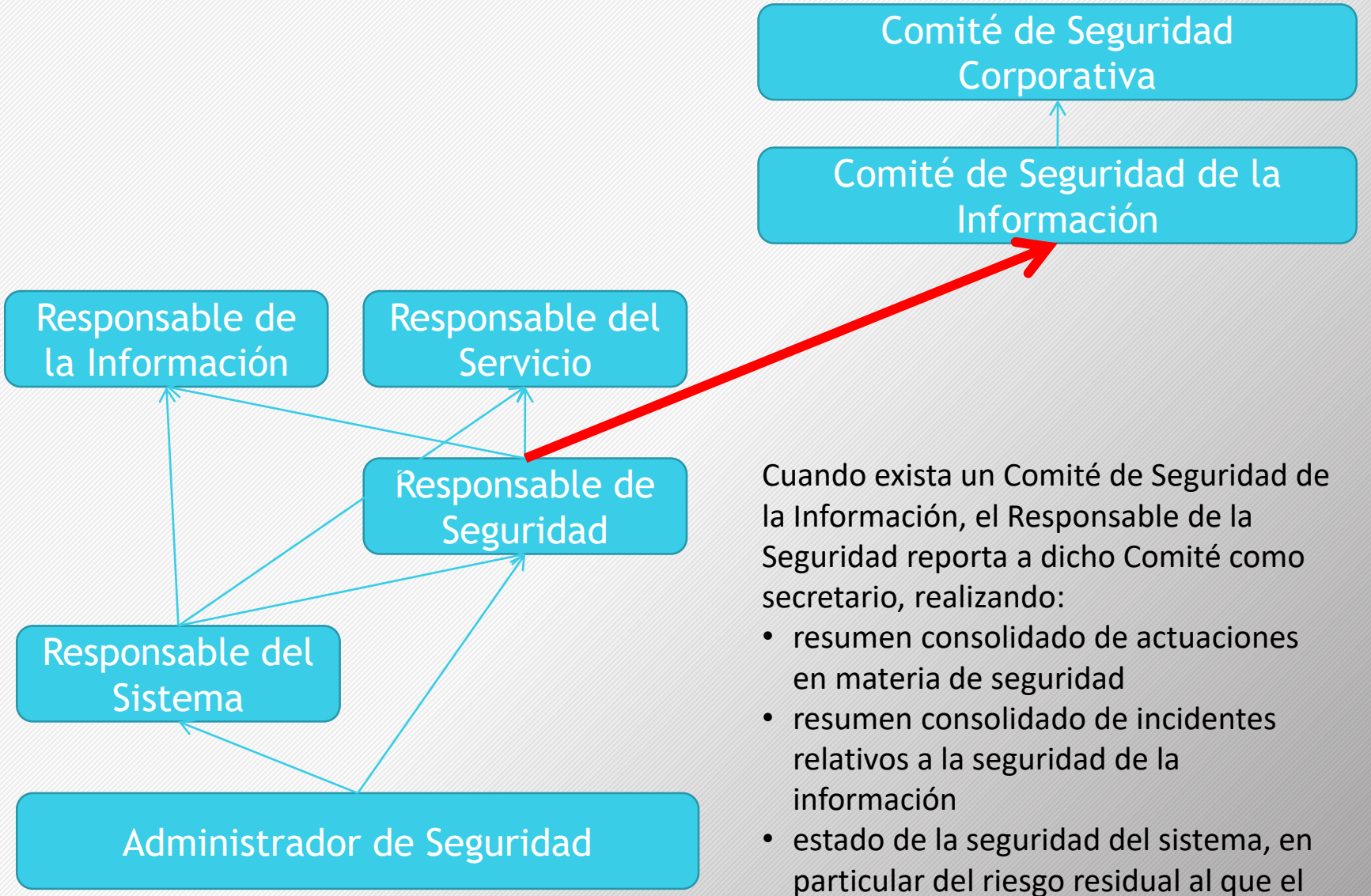
El Responsable del Sistema informa al Responsable de la Información y al Responsable del Servicio de las incidencias funcionales relativas al servicio que le compete.

El Responsable del Sistema reporta al Responsable de la Seguridad:

- actuaciones en materia de seguridad, en particular en lo relativo a decisiones de arquitectura del sistema



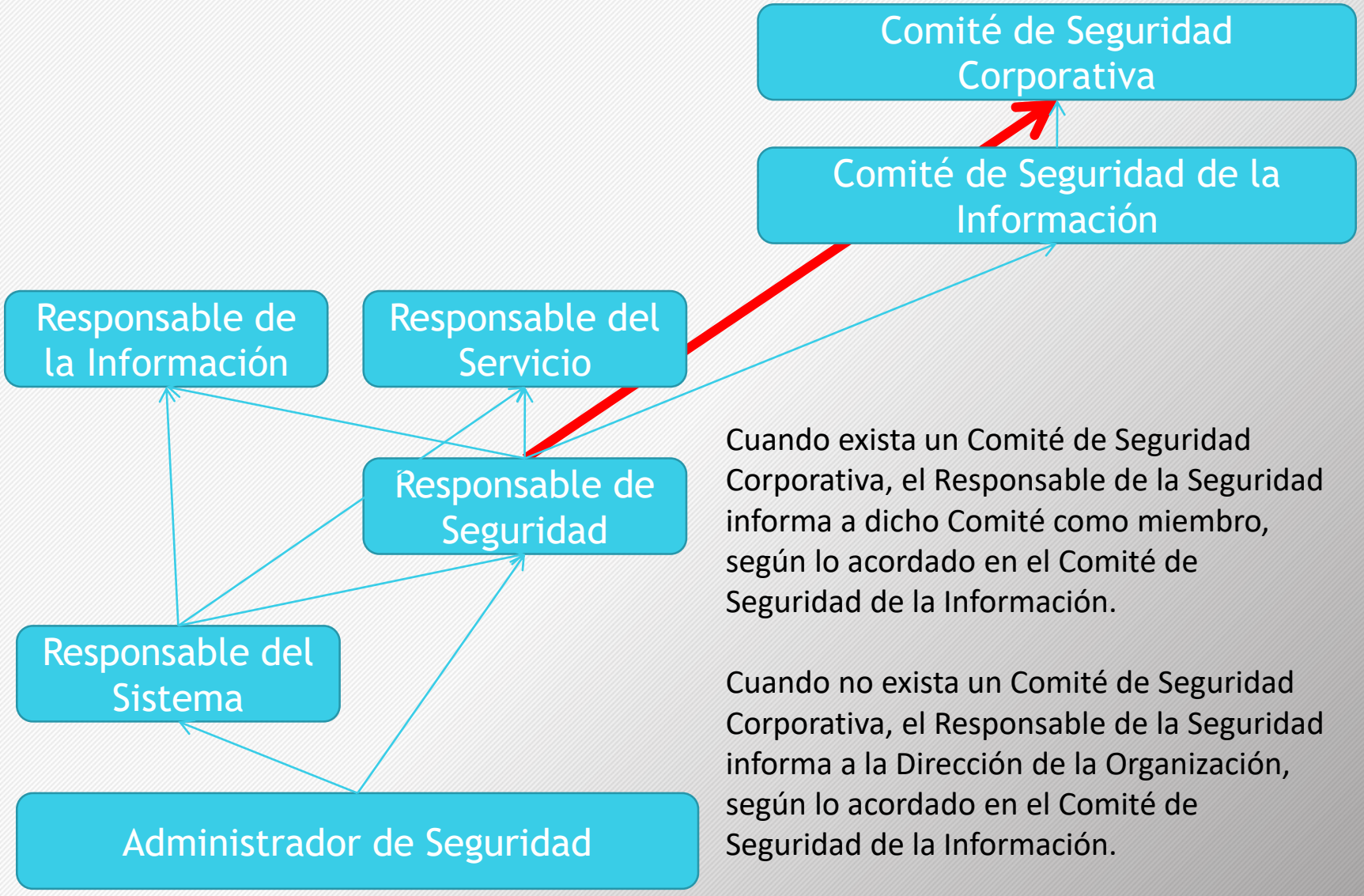
El Responsable de la Seguridad informa al Responsable de la Información y al Responsable del Servicio de las decisiones e incidentes en materia de seguridad que afecten a la información y al servicio, respectivamente, en particular de la estimación de riesgo residual y de las desviaciones significativas de riesgo respecto de los márgenes aprobados.



Cuando exista un Comité de Seguridad de la Información, el Responsable de la Seguridad reporta a dicho Comité como secretario, realizando:

- resumen consolidado de actuaciones en materia de seguridad
- resumen consolidado de incidentes relativos a la seguridad de la información
- estado de la seguridad del sistema, en particular del riesgo residual al que el sistema está expuesto

REPORTES



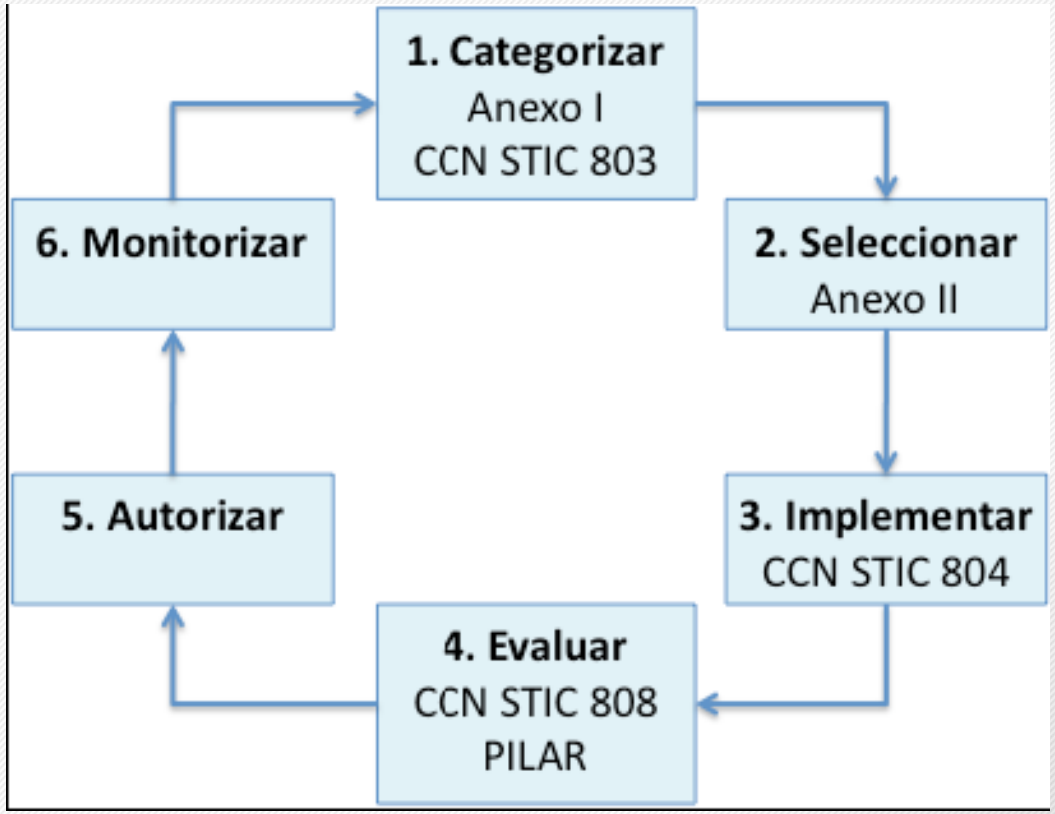
Cuando exista un Comité de Seguridad Corporativa, el Responsable de la Seguridad informa a dicho Comité como miembro, según lo acordado en el Comité de Seguridad de la Información.

Cuando no exista un Comité de Seguridad Corporativa, el Responsable de la Seguridad informa a la Dirección de la Organización, según lo acordado en el Comité de Seguridad de la Información.

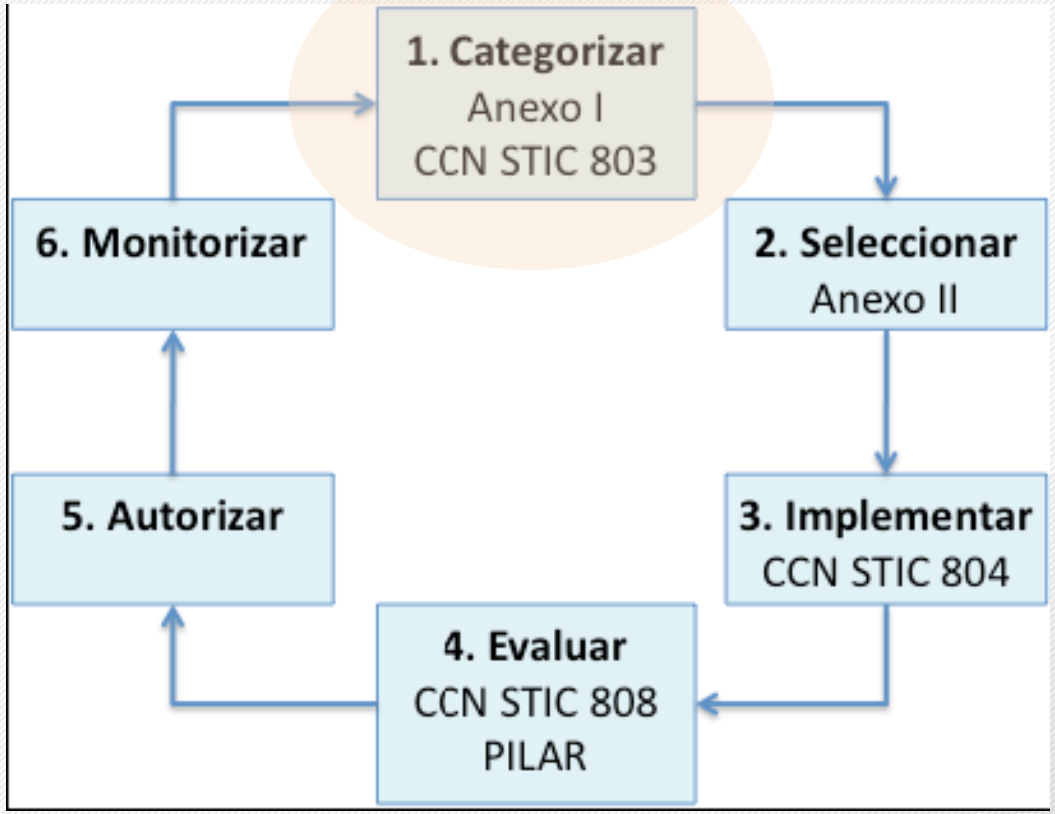
GESTIÓN DE LOS RIESGOS

- El **Responsable de la Información** es el propietario de los riesgos sobre la información.
- El **Responsable del Servicio** es el propietario de los riesgos sobre los servicios.
- El propietario de un riesgo debe ser informado de los riesgos que afectan a su propiedad y del riesgo residual al que está sometida.
- Cuando un sistema de información entra en operación, los riesgos residuales deben haber sido aceptados formalmente por su correspondiente propietario.

La responsabilidad de monitorizar un riesgo recae en su propietario, sin perjuicio de que la función puede ser delegada en el día a día, retomando el control de la situación cuando hay que tomar medidas para atajar un riesgo que se ha salido de los márgenes tolerables.

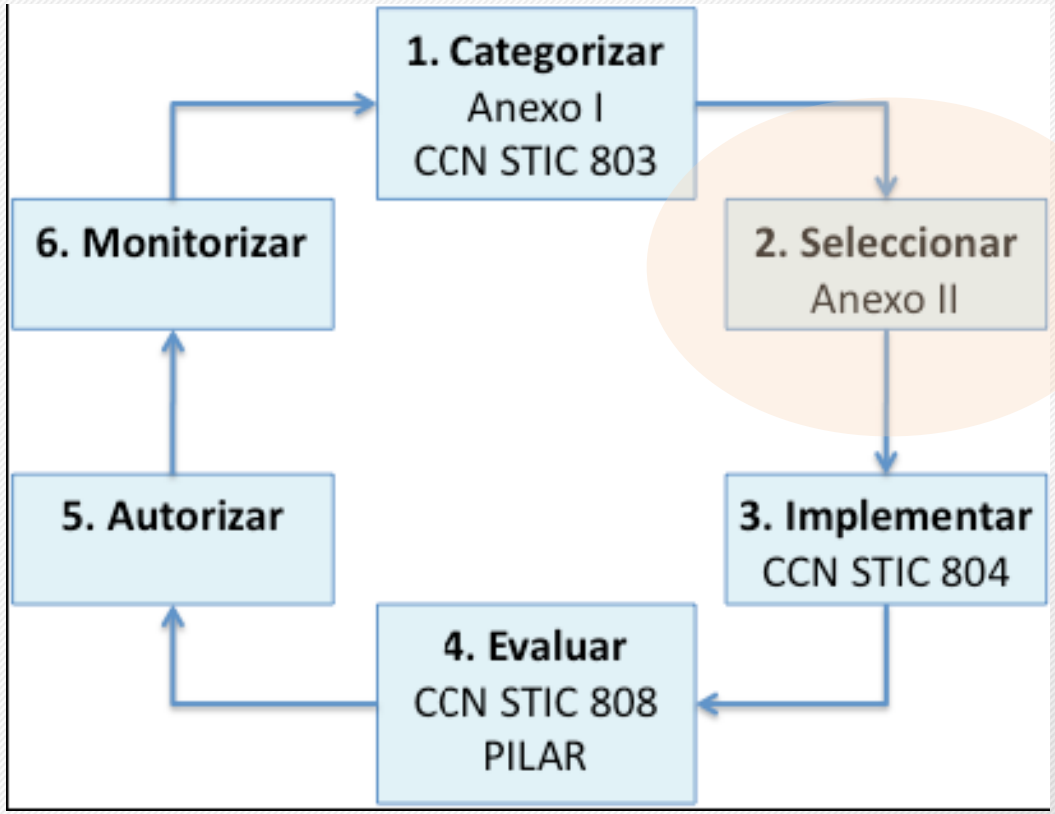


Paso 1 – Categorizar el sistema de información



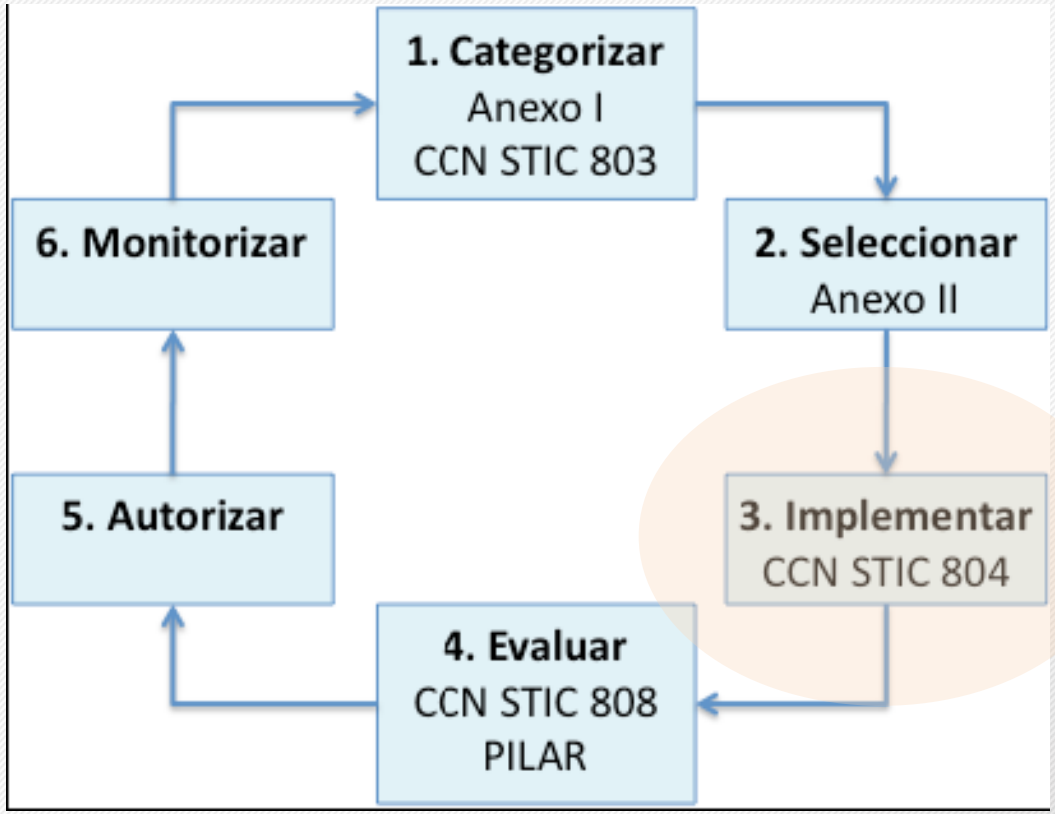
- el Responsable de la Información manejada establece los niveles requeridos (ver Anexo I del ENS y guía CCN-STIC 803)
- el Responsable de los Servicios prestados establece los niveles requeridos (ver Anexo I del ENS y guía CCN-STIC 803)
- se deduce automáticamente la categoría del sistema de información (ver Anexo I del ENS)

Paso 2 – Seleccionar medidas de seguridad



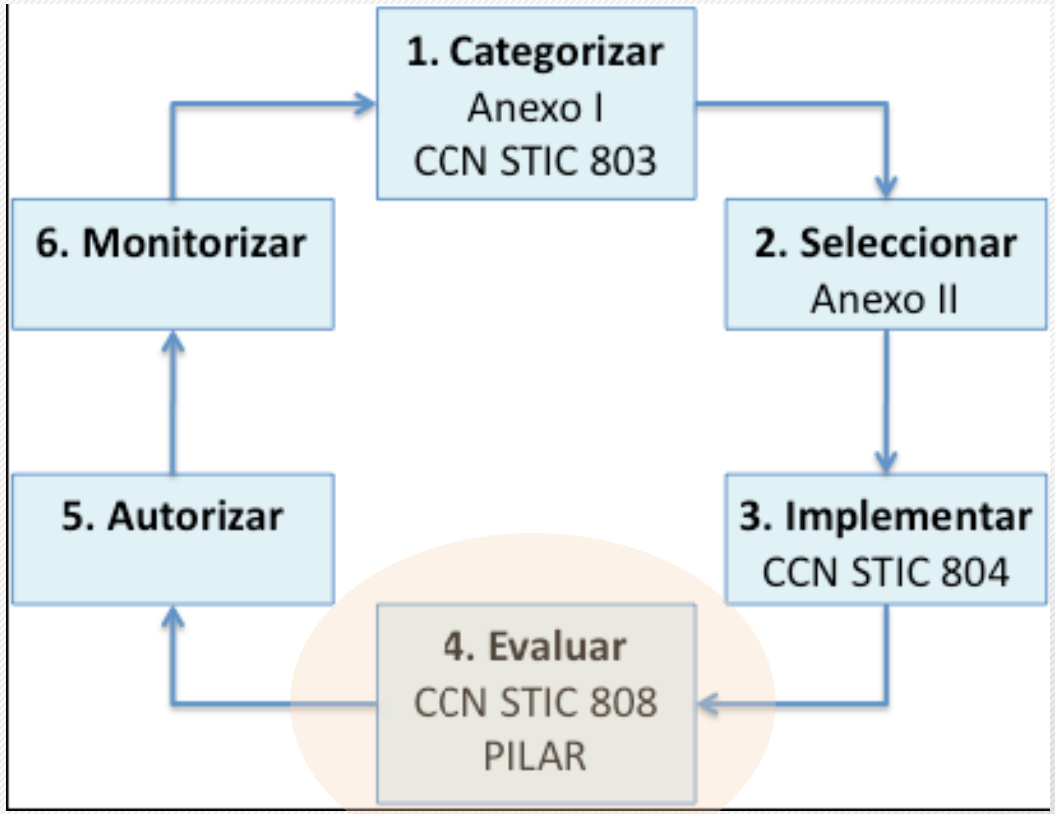
- el Responsable de Seguridad realiza el pertinente análisis de riesgos
- el Responsable de Seguridad determina la Declaración de Aplicabilidad, teniendo en cuenta los mínimos requeridos por el Anexo II del ENS y las medidas adicionales que se estimen oportunas

Paso 3 – Implantar las medidas de seguridad

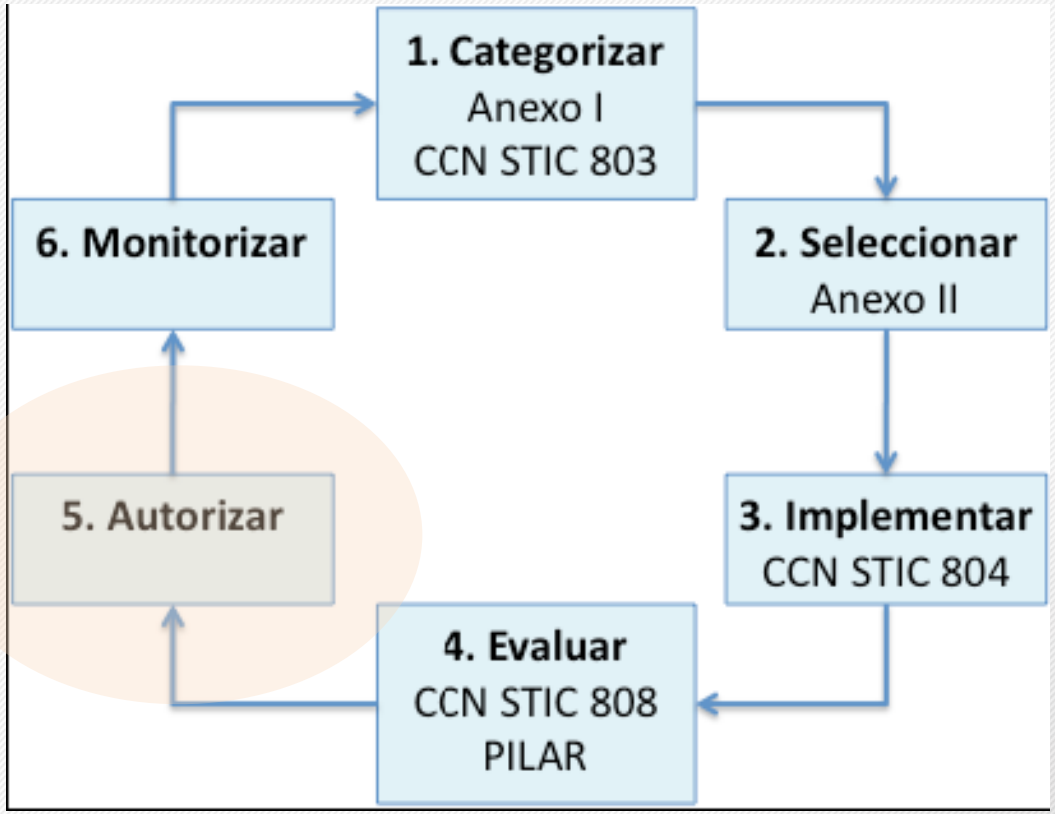


- el Administrador de Seguridad del Sistema (ASS) se encarga de aplicar las medidas acordadas (ver guía CCN STIC 804)

Paso 4 – Evaluar la seguridad del sistema de información

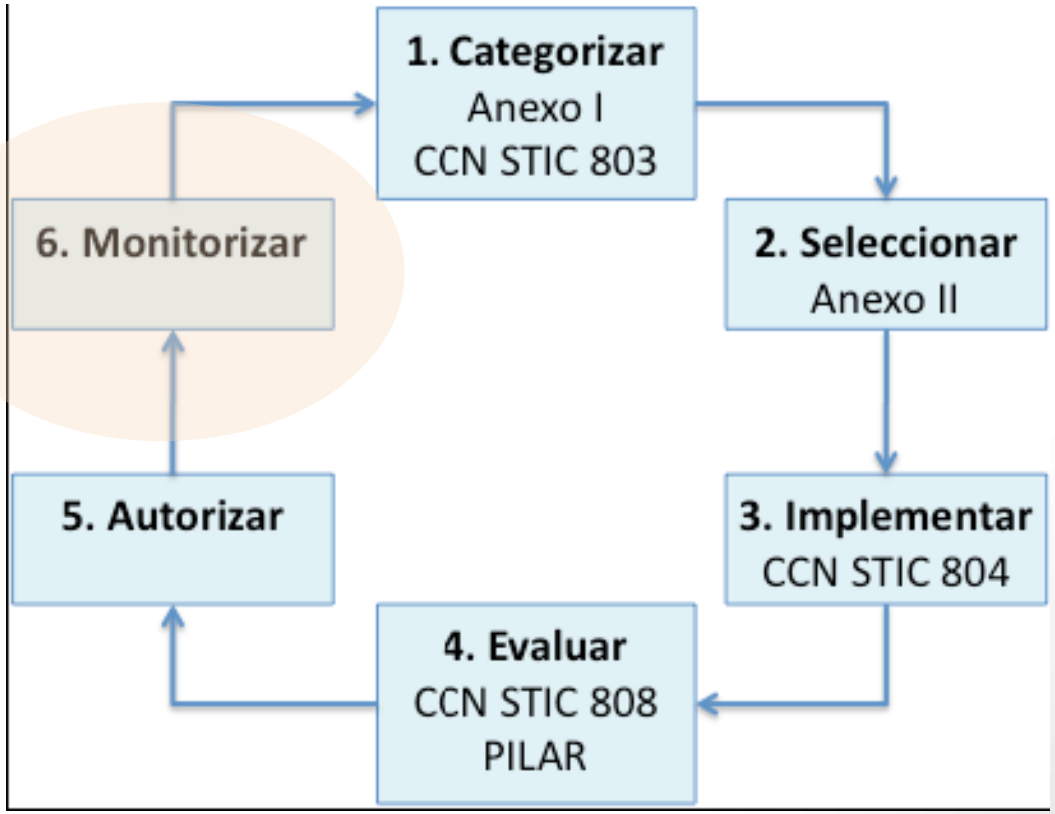


- corresponde al sistema de gestión que se emplee, pudiendo recurrir a auditorías externas cuando sea pertinente (ver guía CCN STIC 802)
- se evalúa el riesgo residual



Paso 5 – Autorización para operar

- el Responsable de la Información acepta el riesgo residual sobre la información que le compete
- el Responsable del Servicio acepta el riesgo residual sobre los servicios que le competen
- puede ser necesario un Plan de Mejora de la seguridad para atender a los riesgos que no son aceptables, regresando al paso 2



Paso 6 – Monitorizar

- el Administrador de Seguridad del Sistema (ASS) recopila información sobre el desempeño del sistema de información en materia de seguridad
- el Responsable de Seguridad monitoriza que el sistema de información se comporta dentro de los márgenes aceptados de riesgo
- los Responsables de la Información y de los Servicios son informados de desviaciones significativas del riesgo sobre los activos de los que son propietarios; si la desviación es elevada, el Responsable del Sistema puede acordar la suspensión temporal del servicio hasta que se puedan garantizar niveles aceptables de riesgo

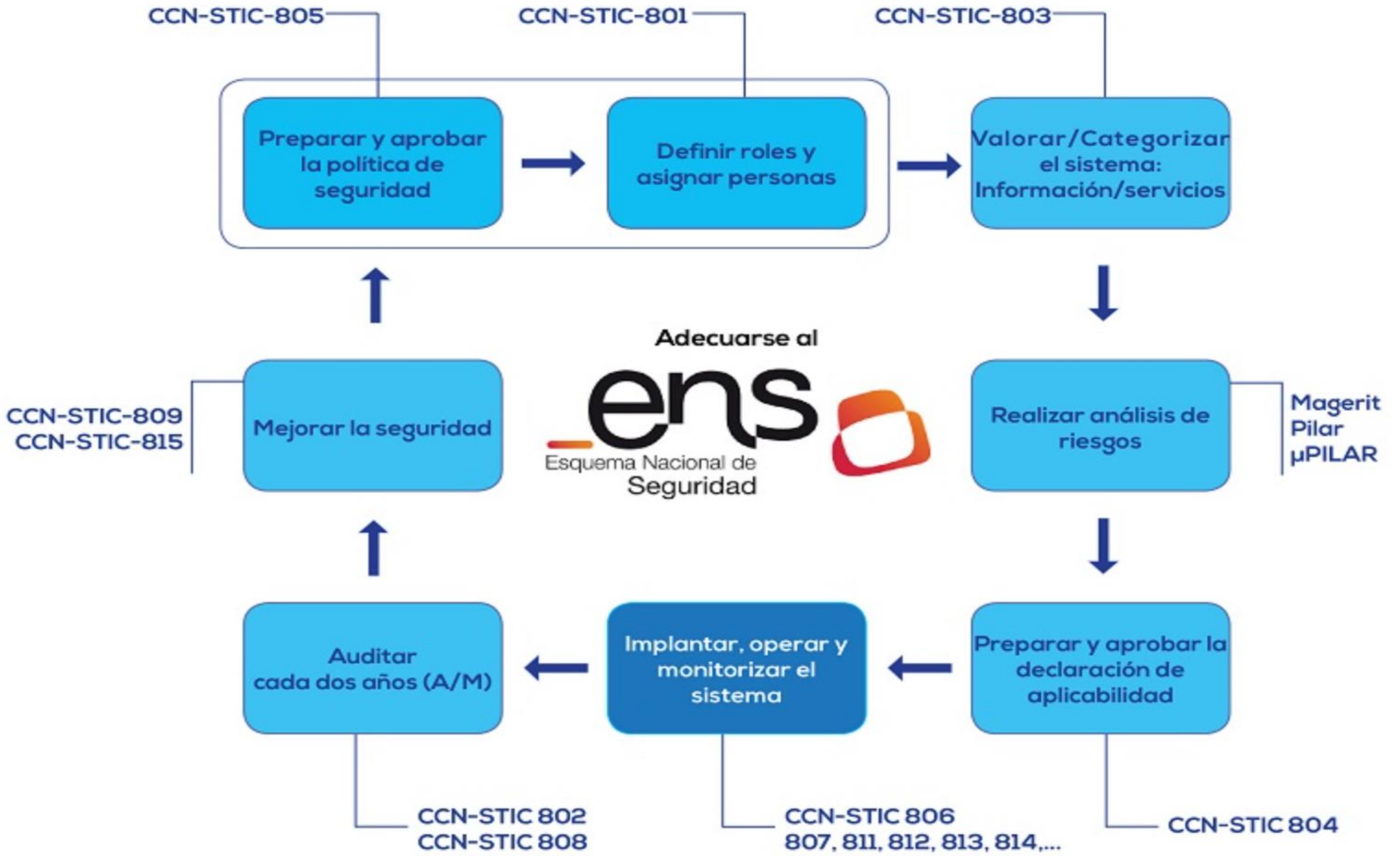
Competencias de las Diputaciones Provinciales

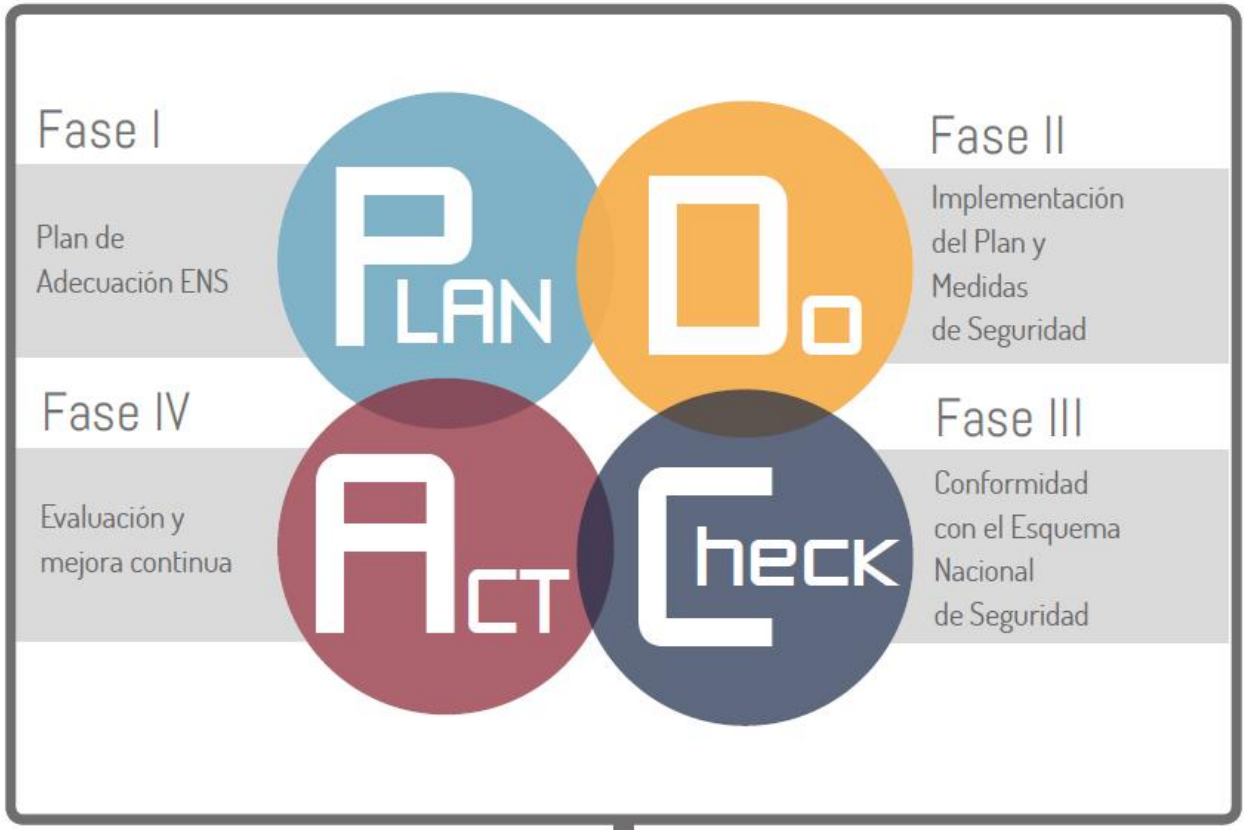
La nueva definición de competencias provinciales establecidas en la Ley 27/2013, de 27 de diciembre, de racionalización y sostenibilidad de la Administración Local, introduce una innovación esencial en relación con la implantación de la Administración Electrónica en los municipios, al atribuir a las diputaciones provinciales, en la nueva redacción dada al artículo 36 de la Ley reguladora de las Bases de Régimen Local, la **competencia para la prestación de los servicios de Administración Electrónica en los municipios con población inferior a 20.000 habitantes, entre ellos el soporte a la implantación del ENS.**

(Confirmada su constitucionalidad por STC 9.6.2016)

(← volver)

Parte III. Diagrama General: Fases Principales





Herramientas CCN-CERT

Guías CCN-STIC

1

PLANIFICACIÓN

Asignación de responsabilidades
Fijación del Contenido del Plan

CCN-STIC-806 Plan de Adecuación al ENS

2

POLÍTICA DE SEGURIDAD

Preparación y aprobación de la Política de Seguridad
Definición de roles y asignación de personas
Modelo de organización de la seguridad

CCN-STIC-805 Política de Seguridad de la Información
CCN-STIC-801 Responsabilidades y Funciones

3

DETERMINACIÓN DE LA CATEGORÍA DEL SISTEMA

Inventario de la Información y los Servicios (implicaciones de protección de datos)
Valorar la información y los servicios de cada una de sus dimensiones (disponibilidad, autenticidad, confidencialidad, integridad y trazabilidad) según "niveles de importancia": Bajo, Medio y Alto.
Valoración de la categoría de los sistemas: Básica, Media y Alta

CCN-STIC-803 Valoración de los sistemas
CCN-STIC-830 Ámbito de aplicación del ENS

ens Esquema Nacional de Seguridad

Plan de Adecuación al ENS

INTRODUCCIÓN

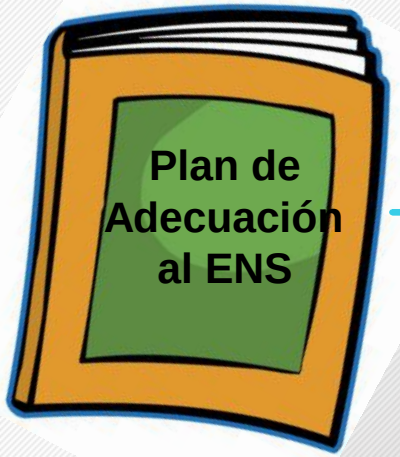
Nuestro Sistema de Información HOY

ADECUACIÓN al ENS

Nuestro Sistema de Información adaptado al ENS

30 de enero de 2011

30 de enero de 2014



- QUÉ hacer.
- CUÁNDO hacerlo.
- DÓNDE hacerlo.
- CÓMO hay que hacerlo.
- QUIÉN lo va a hacer.
- CUÁNTO nos va a costar.

CONTENIDO DEL PLAN DE ADECUACIÓN

1. **Política de Seguridad [+ Normativa Interna de seguridad]**
2. **Información** que se maneja, con su valoración
3. **Servicios** que se prestan, con su valoración
4. **Datos de carácter personal**
5. **Categoría** del sistema
6. **Análisis de Riesgos**
7. **Declaración de Aplicabilidad** de las medidas del Anexo II del ENS y las requeridas por el tratamiento de datos de carácter personal, si los hubiera
8. **Insuficiencias** del sistema *(gap analysis)*
9. **Plan de Mejora de la Seguridad**, incluyendo plazos estimados de ejecución

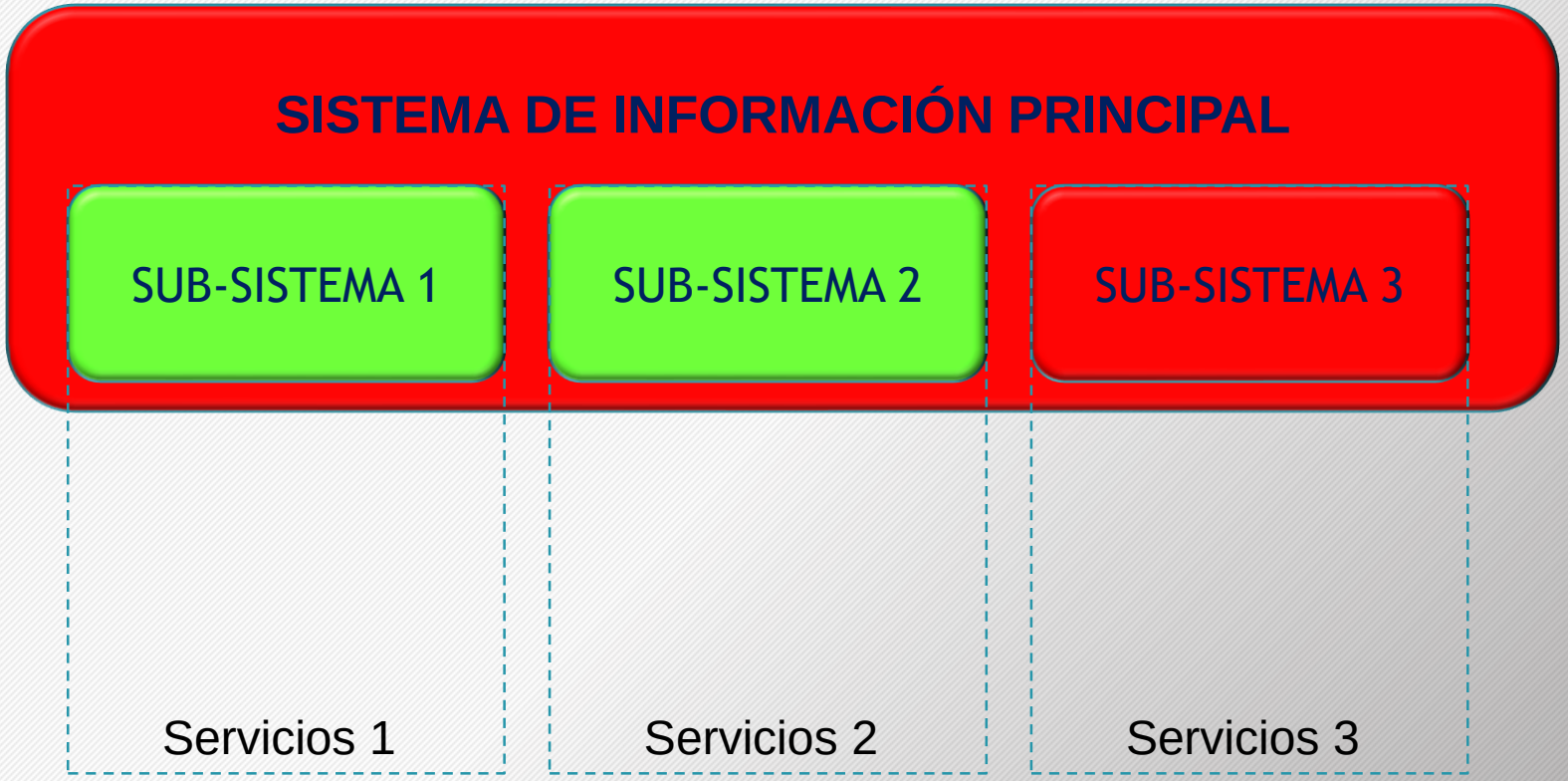
El Plan de Adecuación deberá estar **aprobado por los órganos superiores competentes.**

CONTENIDO DE LA POLÍTICA DE SEGURIDAD

1. Misión u objetivos del organismo	
2. Marco normativo	
3. Organización de seguridad	• Definición de Comités y roles unipersonales • Funciones • Responsabilidades • Mecanismos de coordinación • Procedimientos de designación de personas
4. Concienciación y formación	
5. Postura para la gestión de riesgos	• Plan de Análisis de Riesgos • Criterios de evaluación de riesgos • Directrices de tratamiento • Proceso de aceptación del riesgo residual
6. Proceso de revisión de la Política de Seguridad	

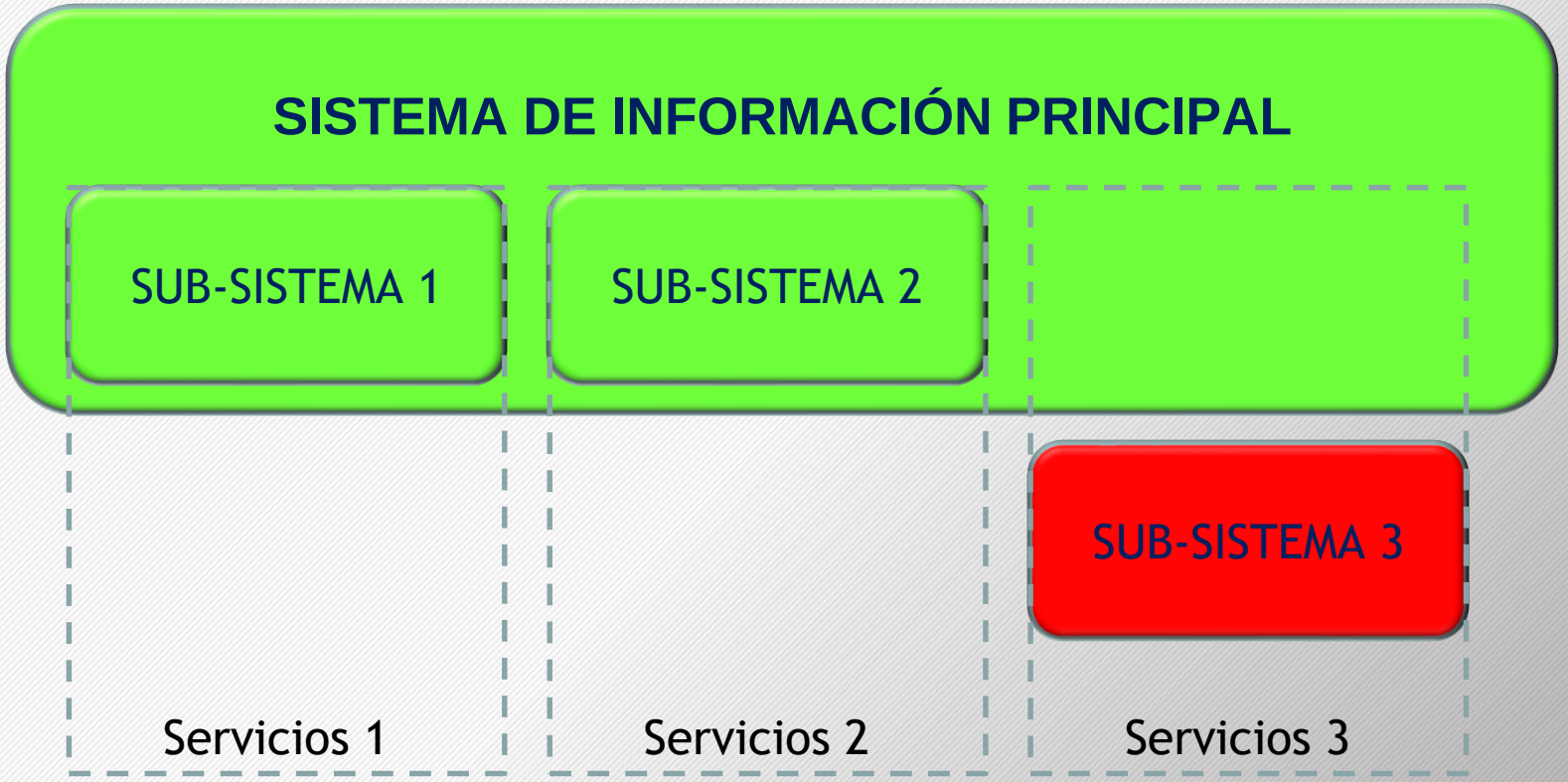
CONTENIDO DEL PLAN DE ADECUACIÓN

CATEGORÍA DEL SISTEMA



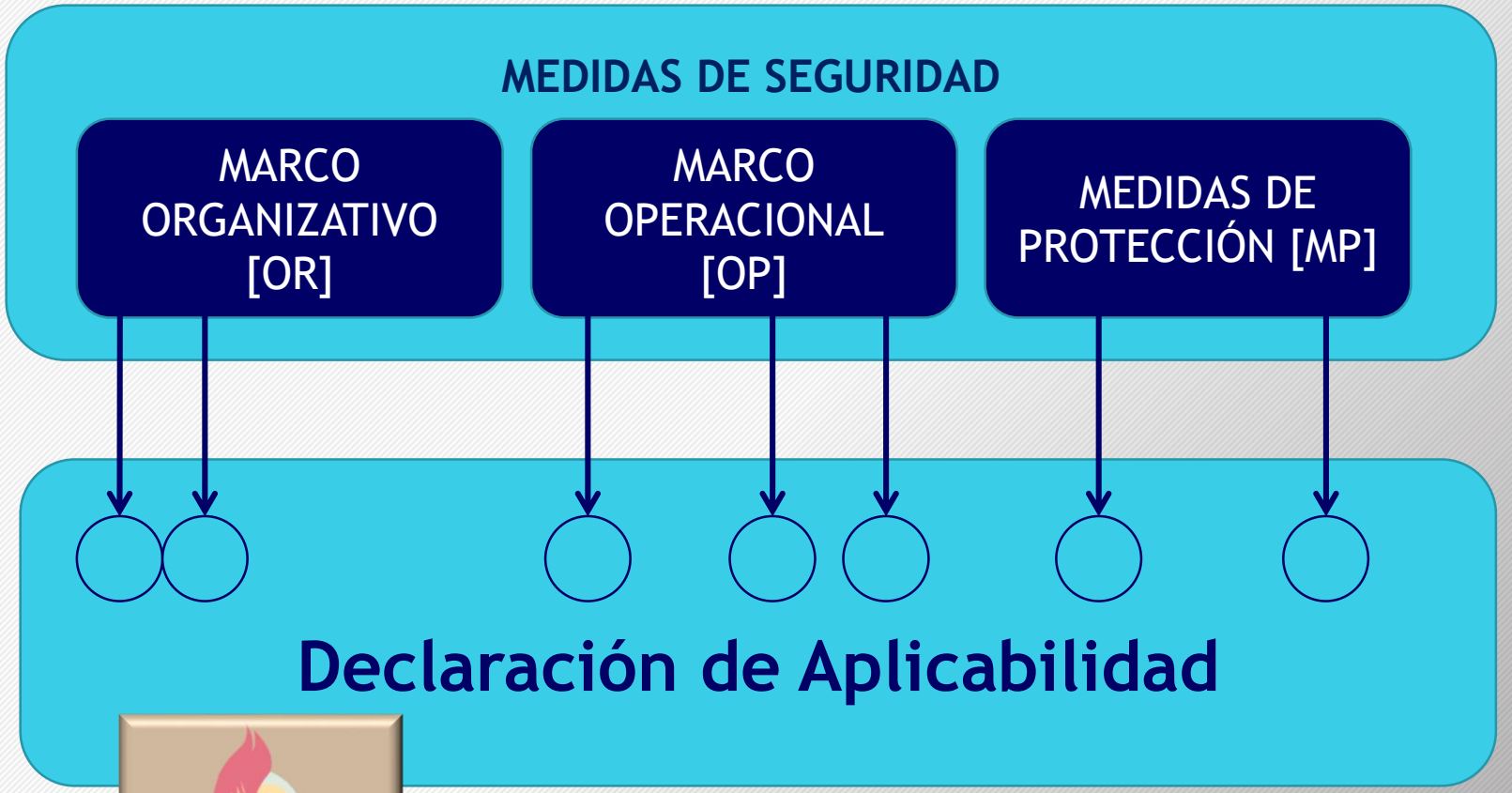
CONTENIDO DEL PLAN DE ADECUACIÓN

CATEGORÍA DEL SISTEMA



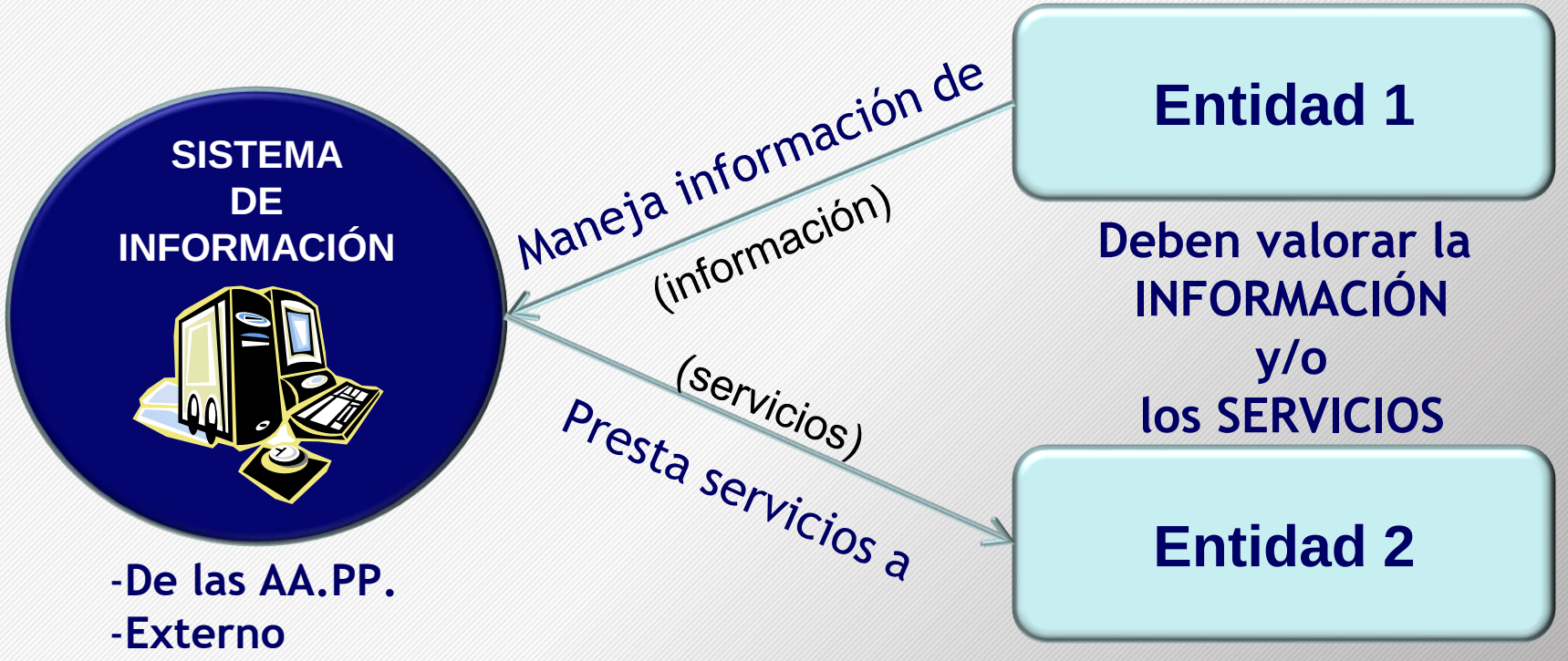
CONTENIDO DEL PLAN DE ADECUACIÓN

DECLARACIÓN DE APLICABILIDAD



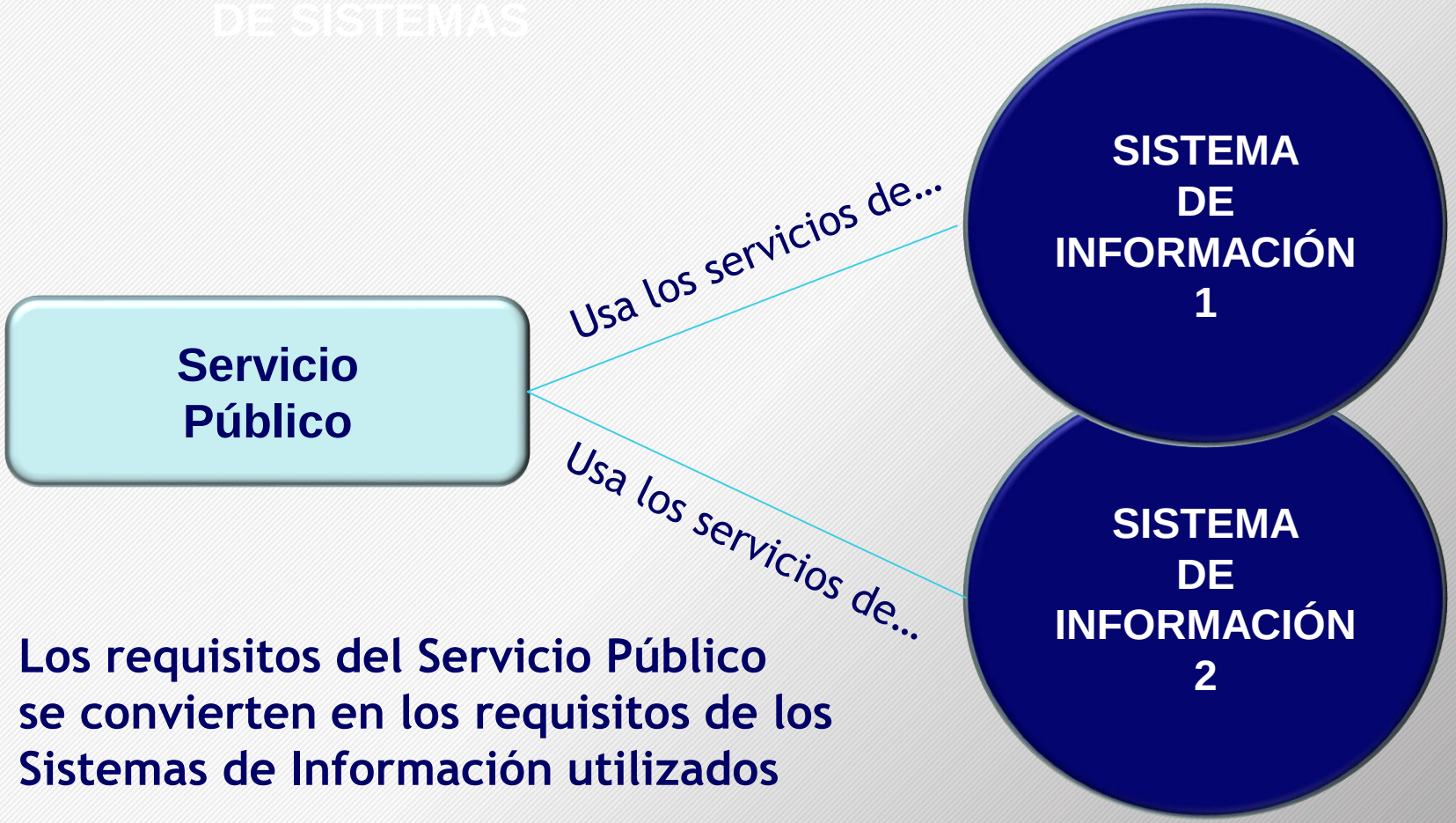
Responsable de Seguridad

4. INTERCONEXIÓN DE SISTEMAS



Los requisitos de otros sistemas que dependen servicios prestados por este sistema, son requisitos de <u>este</u> sistema

4. INTERCONEXIÓN DE SISTEMAS



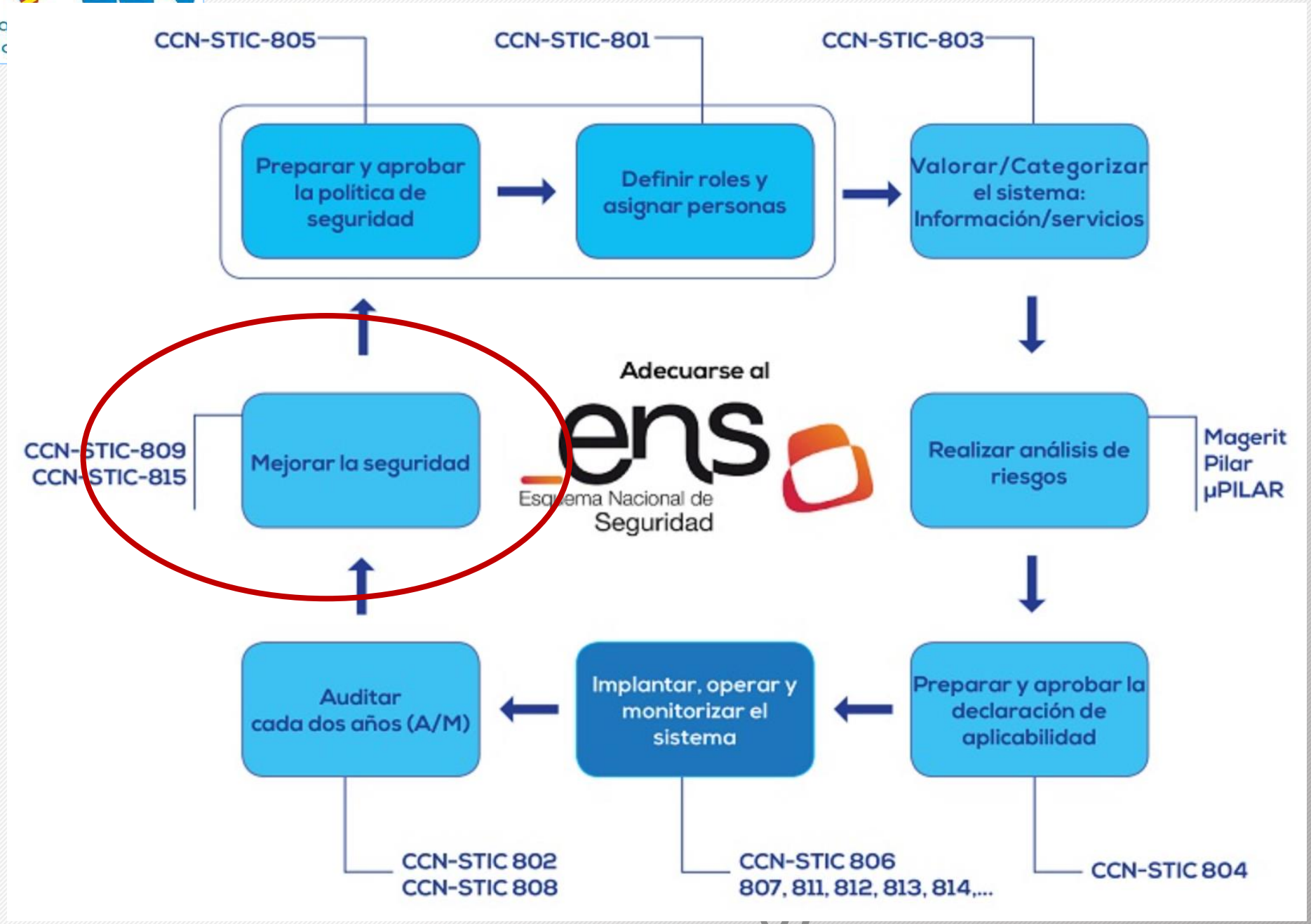
Los requisitos del Servicio Público se convierten en los requisitos de los Sistemas de Información utilizados

regla

- el responsable de la información o servicio puede ser externo
- los requisitos de seguridad los marca el responsable

(← volver)

Parte IV. Conformidad con el ENS


CCN-STIC-805
CCN-STIC-801
CCN-STIC-803
Preparar y aprobar la política de seguridad
Definir roles y asignar personas
Valorar/Categorizar el sistema: Información/servicios
Adecuarse al
ens
Esquema Nacional de Seguridad
CCN-STIC-809
CCN-STIC-815
Mejorar la seguridad
Realizar análisis de riesgos
Magerit
Pilar
µPILAR
Auditar cada dos años (A/M)
Implantar, operar y monitorizar el sistema
Preparar y aprobar la declaración de aplicabilidad
CCN-STIC 802
CCN-STIC 808
CCN-STIC 806
807, 811, 812, 813, 814,...
CCN-STIC 804

El ENS, en su art. 41, señala:

Artículo 41. Publicación de conformidad.

Los órganos y Entidades de Derecho Público darán publicidad en las correspondientes sedes electrónicas a las declaraciones de conformidad, y a los distintivos de seguridad de los que sean acreedores, obtenidos respecto al cumplimiento del Esquema Nacional de Seguridad

- La conformidad de un sistema de información concreto con la norma pasa necesariamente por **adoptar y manifestar que se han adoptado las medidas de seguridad requeridas para tal sistema, atendiendo a su categoría (BÁSICA, MEDIA o ALTA),** y asegurando que tales medidas se mantienen a lo largo de todo el ciclo de vida del sistema.

- Art. 34 → Auditoría de la seguridad.

PROCEDIMIENTOS DE VERIFICACIÓN DE LA CONFORMIDAD

Procedimiento de verificación	Categoría de los Sistemas Afectados	Manifestación de Conformidad	Resultado de la verificación	Análisis de la verificación
AUTOEVALUACIÓN realizada por el mismo personal que administra el sistema de información o aquel otro en quién hubiere delegado.	**BÁSICA**	**DECLARACIÓN DE CONFORMIDAD** 	**Documento de autoevaluación,** indicando si cada medida de seguridad está implantada y sujeta a revisión regular y las evidencias que sustentan la valoración anterior.	Los documentos de autoevaluación serán analizados por el responsable de seguridad competente, que elevará las conclusiones al responsable del sistema para que adopte las medidas correctoras adecuadas.
AUDITORÍA FORMAL con las garantías metodológicas y de independencia, profesionalidad y adecuación requeridas.	**MEDIA / ALTA**	**CERTIFICACIÓN DE CONFORMIDAD** 	**Informe de auditoría,** dictaminando sobre el grado de cumplimiento con el ENS, identificando sus deficiencias y sugiriendo, en su caso, posibles medidas correctoras o complementarias y las recomendaciones que se consideren oportunas. Deberá incluir o referenciar los criterios metodológicos de auditoría utilizados, el alcance y el objetivo de la auditoría, y los datos, hechos y observaciones en que se basen las conclusiones formuladas.	Los informes de auditoría serán analizados por el responsable de seguridad competente, que presentará sus conclusiones al responsable del sistema para que adopte las medidas correctoras adecuadas.


ENAC
Entidad Nacional de Acreditación
INFORMA
CCN-CERT
centro criptológico nacional
ACREDITA
ENTIDAD CERTIFICADORA PRIVADA
ENTIDAD CERTIFICADORA PÚBLICA
AUDITAN Y CERTIFICAN
ENTIDADES PÚBLICAS

Entidades ACREDITADAS / EN PROCESO A 9.10.2017

https://www.ccn-cert.cni.es/ens/entidades-de-certificacion.html

Nombre	Razón social	Enlace web	Estado Acreditación ENS
AENOR Internacional S.A.U.	AENOR Internacional S.A.U.	www.aenor.com	ACREDITADA (21/04/2017)
Audertis Audit Services, S.L.	Audertis Audit Services, S.L.	www.audertis.es	EN PROCESO
BDO Auditores, S.L.P.	BDO Auditores, S.L.P.	www.bdo.es	EN PROCESO
Ingeniería de Sistemas para la Defensa de España (ISDEFE)	Empresa pública de consultoría e ingeniería	www.isdefe.es	-
LEET Security, S.L.	LEET Security, S.L.	www.leetsecurity.com	EN PROCESO
LGAI Technological Center, S.A.	LGAI Technological Center, S.A.	www.appluscertification.com/es	EN PROCESO

DECLARACIÓN DE CONFORMIDAD

CON EL RD 3/2010, DE 8 DE ENERO, POR EL QUE SE REGULA EL ESQUEMA NACIONAL DE SEGURIDAD EN EL ÁMBITO DE LA ADMINISTRACIÓN ELECTRÓNICA

(ENS)

Logotipo de la Entidad Pública declarante	*Identificación inequívoca del declarante, incluyendo la denominación legal que aprueba la estructura orgánica a la que está adscrito.*

Los sistemas de información reseñados seguidamente, todos ellos de categoría BÁSICA, y conforme a lo dispuesto en el Anexo III del RD 3/2010, han superado un proceso de autoevalución realizado en las fechas que se indican:

1.	*aaaa/mm/dd*	*Denominación Sistema de Información 1 y servicios prestados*
2.	*aaaa/mm/dd*	*Denominación Sistema de Información 2 y servicios prestados*
...	*...*	*...*

Dicho proceso de autoevaluación garantiza que los sistemas referenciados cumplen las medidas de seguridad impuestas por el RD 3/2010, para sistemas de categoría BÁSICA.

En *Localidad*, **a** ___ **de** _____ **de 20**__

Fdo. *Nombre y Apellidos del titular del*

Órgano Superior de que se trate

Administración Pública de que se trate

Evidencias de

Firma electrónica [personal / para actuación administrativa automatizada]

del declarante

centro nacional de inte
centro criptológico n

Agencia de Tecnología Legal

Logotipo de la Entidad Certificadora

CERTIFICACIÓN DE CONFORMIDAD CON EL ens Esquema Nacional de Seguridad

Categoría [BÁSICA/MEDIA/ALTA]

aaaa / mm / dd
Número del certificado: _____

Certificación

Concedida a

Entidad(1)

Población

Dirección postal

Entidad Certificadora **certifica que el Sistema de Información *Denominación del Sistema de Información*, de categoría _____ (2), ha sido auditado y encontrado conforme con las exigencias del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración electrónica.**

Los servicios prestados por el antedicho Sistema de Información son: _____
_____

Declaración de aplicabilidad: versión ___, fecha: ___ de _____ de 201_

Fecha de certificación inicial: ___ de _____ de 201_
Fecha de expiración: ____ de _____ de 201_ (3).

Para cualquier aclaración sobre el alcance del presente certificado y la aplicación de los requisitos del ENS, pueden ponerse en contacto con la *Entidad Certificadora*.

Número del Certificado: _____
Fecha: ___ de _____ de 201_
Firma *del responsable de la Entidad Certificadora:*

Nombre completo /razón social de la Entidad Certificadora y pág. web.
Dirección postal / electrónica.
Oficina de emisión (en su caso).
Código Postal. Provincia. País.

SOLUCIONES Y SERVICIOS PRESTADOS POR EL SECTOR PRIVADO

- Es muy frecuente que los **operadores del sector privado** participen en la **prestación de servicios a las entidades públicas** (como los servicios en la nube, por ejemplo), actividades a las que, en muchos casos, les resulta de aplicación lo dispuesto en el ENS.

- Tales operadores económicos, cuando presten servicios a los que resulte exigible el cumplimiento del ENS, deben **exhibir la correspondiente Declaración de Conformidad / Certificación de Conformidad**, utilizando los mismos procedimientos que los exigidos para las entidades públicas.

- Cuando sea necesario, es responsabilidad de las entidades públicas notificar a dichos operadores económicos la **necesidad de que los servicios sean conformes con lo dispuesto en el ENS** y posean las correspondientes **Declaraciones o Certificaciones de Conformidad**, según lo señalado en la Guía CCN-STIC 809.

Caminante, son tus huellas
el camino, y nada más;
caminante, no hay camino,
se hace camino al andar.

(A. Machado. Proverbios y Cantares, XXIX)

Con la ciberseguridad pública…
sucede lo mismo.

Muchas gracias

cgalan@atl.es