sedian

Seguridad Digital
de Andalucía

Esquema Nacional de Seguridad (Cuestiones de implantación)

28 de Octubre de 2022

Junta de Andalucía

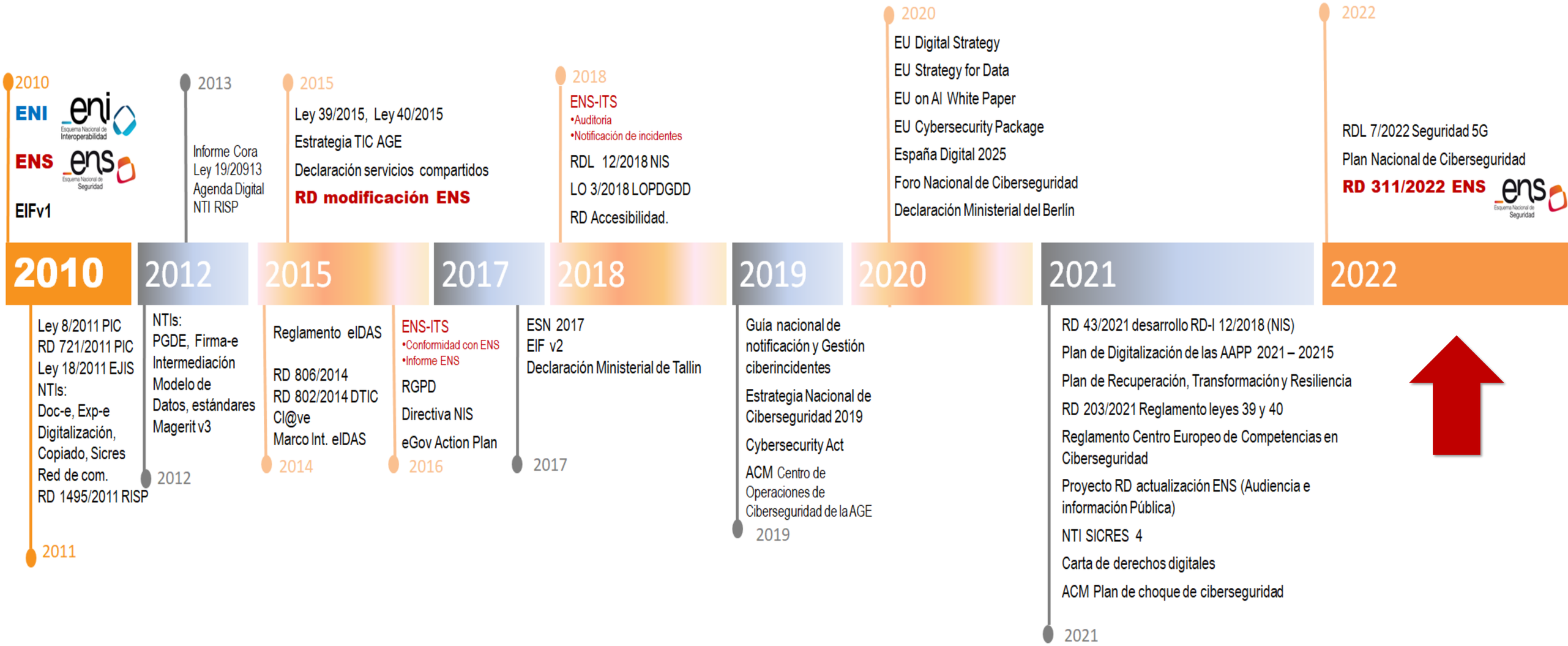
Dr. Carlos Galán

- **Licenciado y Doctor en Informática, Licenciado en Derecho y Abogado especialista en Derecho de las TIC.**
- **Profesor de *Derecho de las TIC* en la Universidad Carlos III de Madrid (Área de Derecho Administrativo) y de *Aspectos Legales de la Ingeniería Informática* (Área de Ingeniería Informática).**
- **Asesor del CCN-CERT.**
- **Miembro de la European Artificial Intelligence Alliance.**
- **Miembro del Grupo de Trabajo de Ciberpolítica del Real Instituto Elcano.**
- **Miembro del Grupo de Trabajo de Formación, Capacitación y Talento del Foro Nacional de Ciberseguridad.**
- **Miembro del Grupo de Expertos para el desarrollo de la Estrategia de Ciberseguridad Nacional, en 2013 y 2019.**
- **Miembro del equipo de redacción del ENS.**

Índice

El nuevo ENS (RD 311/2022)

ENS – Dónde estamos



ENS – Desarrollo

Base legal

- ✓Real Decreto 3/2010
- ✓Actualizado en 2015
- ✓**Real Decreto 311/2022**
- ✓Anclado en leyes 40/2015 y 39/2015
- ✓ + Instrucciones Técnicas de Seguridad

Ámbito de aplicación

- ✓Sector Público
- ✓Información clasificada
- ✓Proveedores

Referente

- ✓ Ley Orgánica 3/2018
- ✓ Real Decreto 43/2021

4 ITS publicadas

- ✓ Informe estado de a seguridad
- ✓ Conformidad con el ENS
- ✓ Auditoría
- ✓ Notificación de incidentes

Conformidad

- ✓Acreditación con ENAC
- ✓ Certificadores acreditados por ENAC
- ✓ Entidades certificadas (públicas/privadas)
- ✓ Consejo de Certificación del ENS (CoCENS)

Monitorización - Informe INES

- ✓ 8 ediciones del informe INES

Soporte

- ✓ >90 **guías** CCN-STIC Serie 800
- ✓ 23 **Soluciones de** ciberseguridad

sedian Seguridad Digital de Andalucía

ENS – Por qué la actualización

Intensificación de las ciberamenazas y ciberincidentes

Progreso de la transformación digital con impacto global

Avance de las tecnologías

Evolución del marco legal

Evolución del marco estratégico en ciberseguridad

Extensión de la implantación del ENS

Acumulación de experiencia de aplicación del ENS

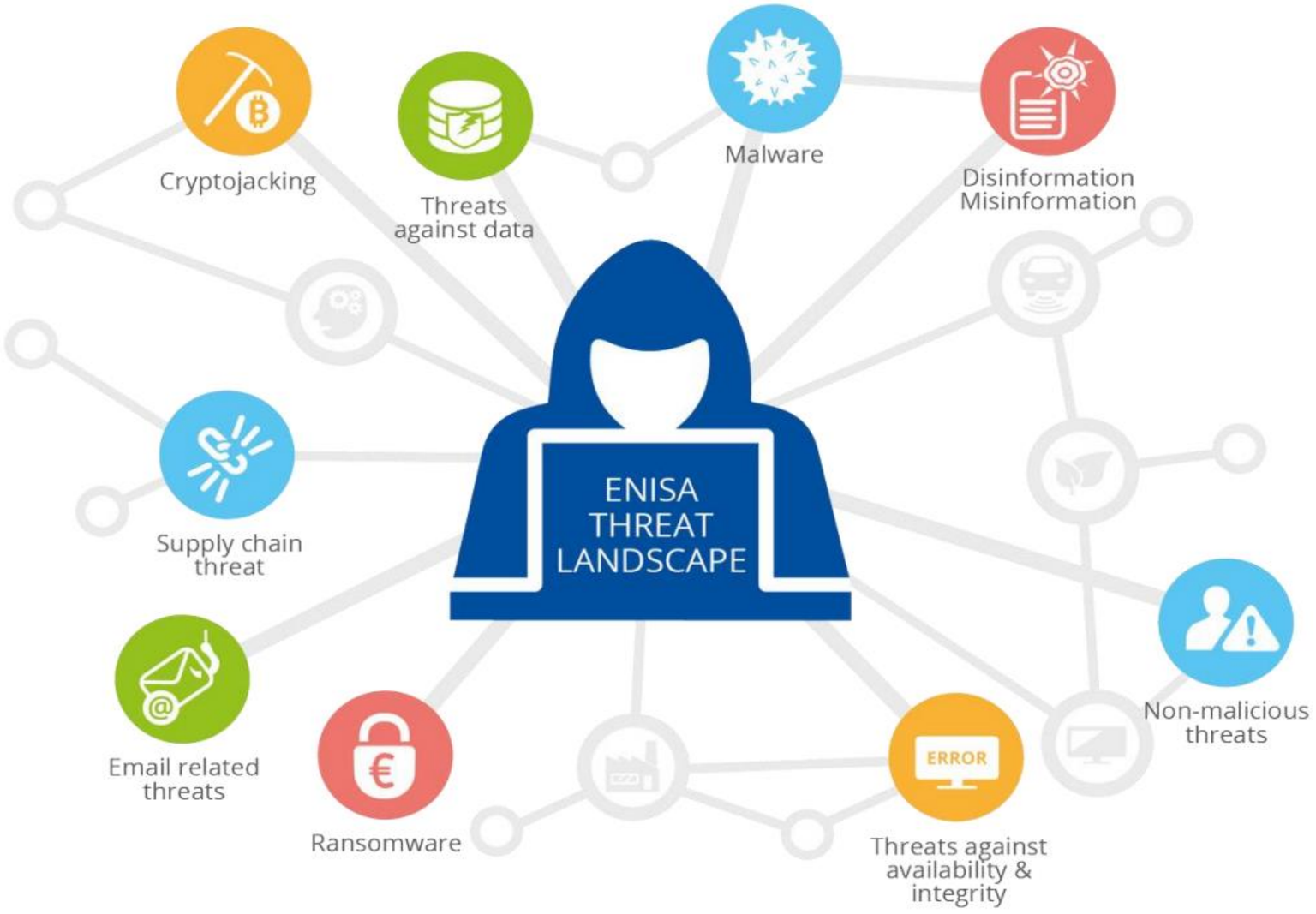
Mejor conocimiento del estado de la seguridad nacional (informe INES)

Mayor volumen de guías y servicios del CCN-CERT

Fuente: Infografías ENS

Panorama de amenazas

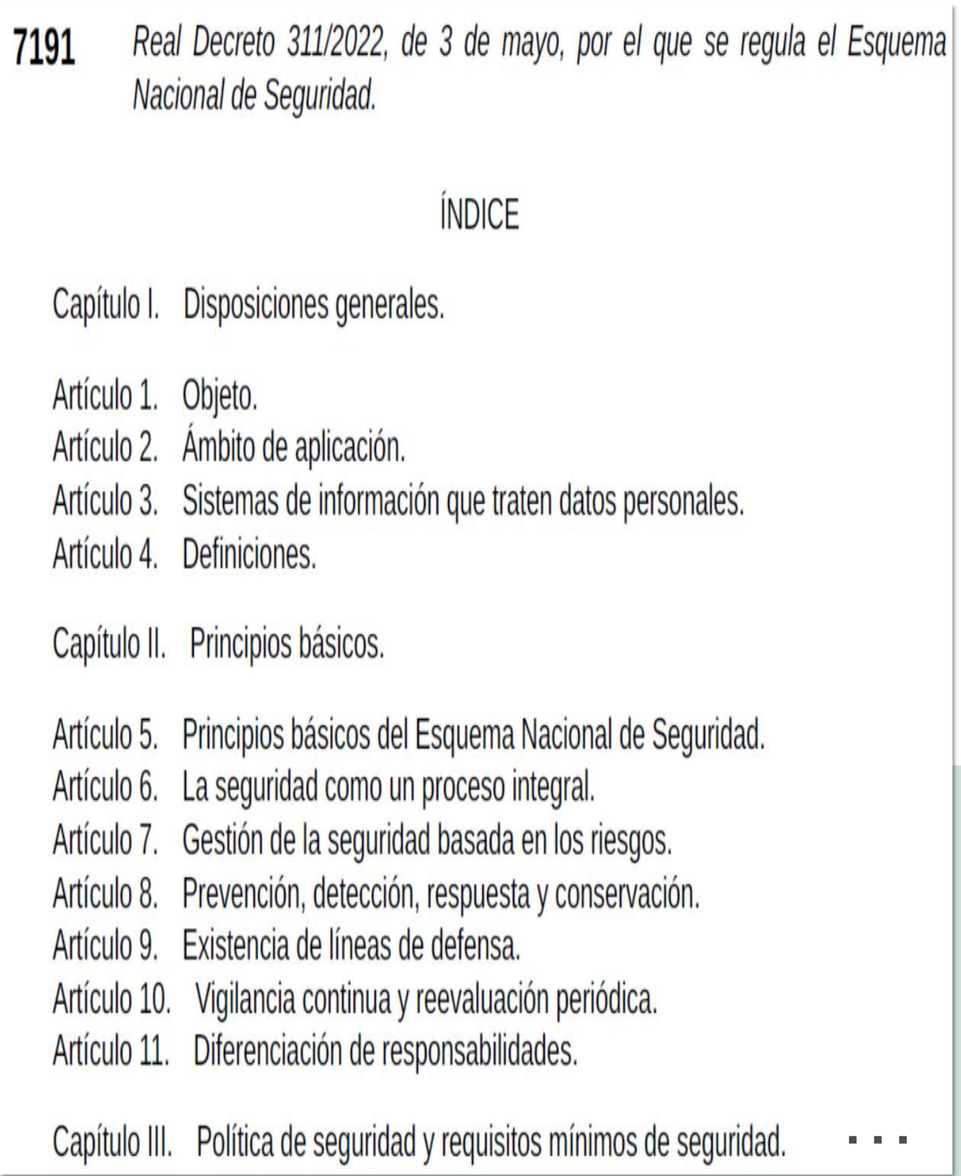
Figure 1: ENISA Threat Landscape 2021 - Prime threats



ENS – Objetivos de la actualización

1. **Mejorar y alinear el ENS con el nuevo marco legal y estratégico** para facilitar la seguridad de la administración digital
2. **Introducir la capacidad de ajustar los requisitos del ENS** para una aplicación más eficaz y eficiente
3. **Revisar de forma pormenorizada principios, requisitos y medidas para facilitar la adaptación** a tendencias y necesidades en ciberseguridad

RD 311/2022 – El nuevo ENS, en cifras



7191 *Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.*

ÍNDICE

- ✓ A la escucha **desde 2015**, por todos los canales
- ✓ En preparación **desde 2019**
- ✓ **445** Observaciones (audiencia e información pública)
- ✓ **9** Informes

- ✓ **34.900** Palabras (frente a 20.500 de v2015)
- ✓ **90** Páginas
- ✓ **7** Capítulos, **41** Artículos, **3** dd.aa.; **1** d.t.; **1** d.d.u.; **4** dd.ff., **4** Anexos
- ✓ **7** Principios básicos
- ✓ **15** Requisitos mínimos
- ✓ **73** Medidas de seguridad

RD 311/2022 - Panorámica

1. **Disposiciones generales**, **objeto, ámbito de aplicación**, … (arts. 1 – 4)
2. **Principios básicos**, que sirven de guía. (arts. 5 – 11)
3. **Requisitos mínimos**, de obligado cumplimiento. (arts. 12 – 27)
4. **Categorización de los sistemas** para la adopción de **medidas de seguridad** proporcionadas. (arts. 28, 40, 41, A-I y A-II)
5. Uso de **productos certificados**. Papel del Organismo de Certificación (OC-CCN) (art. 19 y A-II)
6. Uso de **infraestructuras y servicios comunes** (art. 29)
7. Los **perfiles de cumplimiento específicos** (art. 30)
8. La **auditoría de la seguridad** que verifique el cumplimiento del ENS. (art. 31)
9. **Informe del estado de la seguridad** (art. 32)
10. **Respuesta a incidentes de seguridad** (arts. 33 y 34)
11. La **conformidad con el ENS** (art. 38)
12. La **formación** (D.a. 1ª)
13. Las **instrucciones técnicas de seguridad** (D.a. 2ª)
14. Las **guías de seguridad** (D.a. 2ª)

Fuente: Infografías ENS

Disposición transitoria única:
Adecuación de sistemas -> **24 meses**

RD 311/2022 – Ámbito de aplicación claro (arts. 2, 3)

Photo by Marvin Meyer on Unsplash

- ✓ **Todo el sector público** según artículo 2 de la Ley 40/2015.
- ✓ Sistemas que tratan **información clasificada**.
- ✓ **Entidades del sector privado** cuando presten servicios o provean soluciones.
- ✓ Los **pliegos de prescripciones** contemplarán los requisitos de conformidad con el ENS.
- ✓Referencia a la instalación, despliegue, explotación de redes **5G** o prestación de servicios 5G por entidades del sector público.
- ✓ Sistemas de información que traten **datos personales**.

RD 311/2022 – Perfiles de cumplimiento (art. 30)

Photo bClaudio Schwarz | @purzlbaum on Unsplash

✓Comprenderán aquel conjunto de medidas de seguridad que resultando del preceptivo análisis de riesgos, resulten idóneas para una concreta categoría de seguridad.

✓Persiguen introducir la capacidad de **ajustar los requisitos del ENS a necesidades específicas de determinados**

- ✓**Colectivos**: Entidades Locales, Universidades, Organismos Pagadores, …
- ✓**Ámbitos tecnológicos**: servicios en la nube, …

Ej:
- ✓ CCN-STIC-881A. Perfil de Cumplimiento Específico Universidades
- ✓ CCN-STIC-883 Guía de implantación del ENS para Entidades Locales
- ✓ …

RD 311/2022 – Respuesta a incidentes (art. 33)

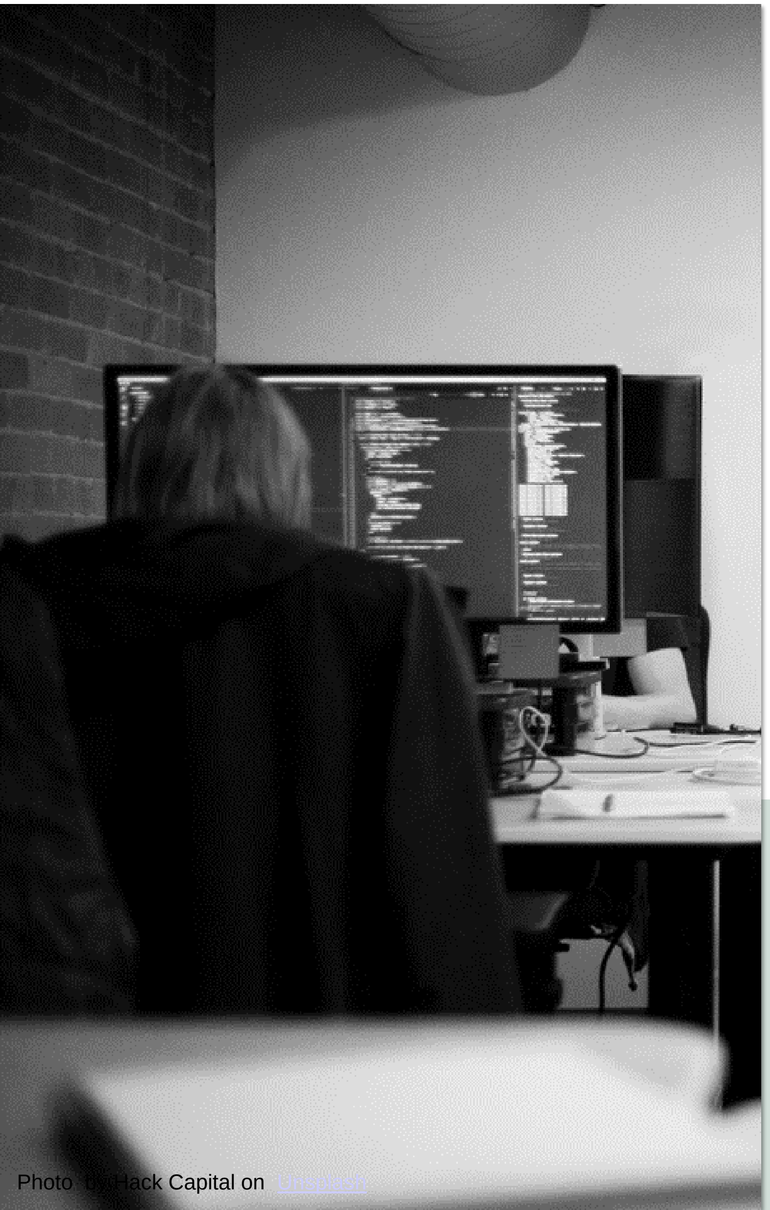
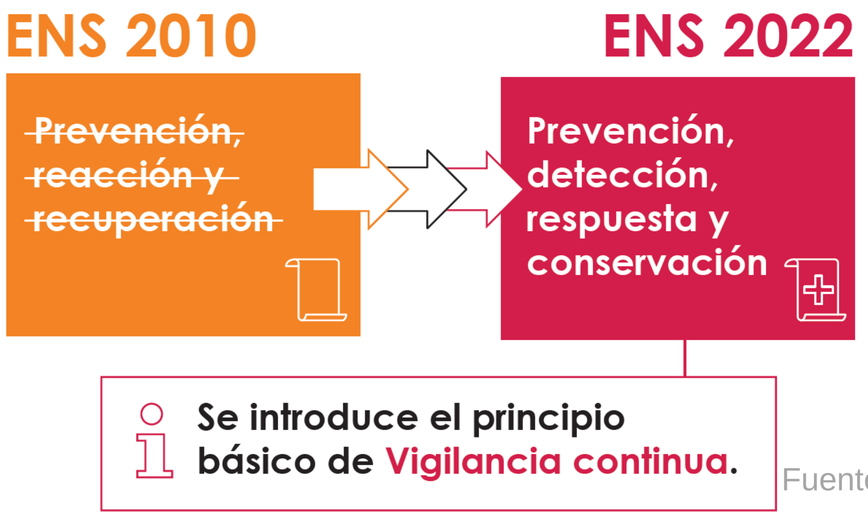
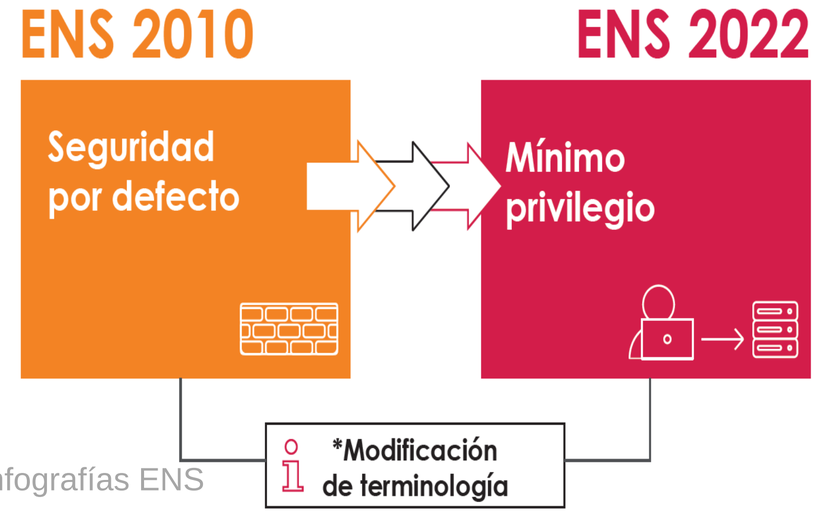


Photo by Hack Capital on Unsplash

- ✓**Las entidades públicas notificarán al CCN-CERT** los incidentes de seguridad.
- ✓**Las organizaciones del sector privado** que presten servicios a las entidades públicas **notificarán al INCIBE-CERT** quien lo pondrá inmediatamente en conocimiento del **CCN-CERT**.
- ✓El **CCN-CERT determinará técnicamente el riesgo de reconexión** de sistemas afectados, indicando procedimientos a seguir y salvaguardas a implementar.
- ✓La **SGAD autorizará la reconexión** a medios y servicios comunes en su ámbito de responsabilidad, **si un informe de superficie de exposición del CCN-CERT** determina que el riesgo es asumible.
- ✓Papel de otros actores: Coordinación con el **Ministerio del Interior** a través de la **OCC** (RD-l 12/2018); **ESPDEF-CERT**; **IGAE**.

RD 311/2022 – Principios y requisitos





Fuente: Infografías ENS

a) Seguridad como proceso integral.
b) Gestión de la seguridad basada en los riesgos.
c) Prevención, detección, respuesta y conservación
d) Existencia de líneas de defensa.
e) Vigilancia continua
f) Reevaluación periódica.
g) Diferenciación de responsabilidades.

Política de seguridad y requisitos mínimos de seguridad
Organización e implantación del proceso de seguridad

a) Organización e implantación del proceso de seguridad.
b) Análisis y gestión de los riesgos.
c) Gestión de personal.
d) Profesionalidad.
e) Autorización y control de los accesos.
f) Protección de las instalaciones.
g) Adquisición de productos de seguridad y contratación de servicios de seguridad.
h) Mínimo privilegio.
i) Integridad y actualización del sistema.
j) Protección de la información almacenada y en tránsito.
k) Prevención ante otros sistemas de información interconectados.
l) Registro de la actividad y detección de código dañino.
m) Incidentes de seguridad.
n) Continuidad de la actividad.
ñ) Mejora continua del proceso de seguridad.

RD 311/2022 – Medidas de seguridad

Marco organizativo: medidas relacionadas con la organización global de la seguridad

Marco operacional: medidas para proteger la operación del sistema como conjunto integral de componentes para un fin.

Medidas de protección: para proteger activos concretos, según su naturaleza, con el nivel requerido, en cada dimensión de seguridad.

Fuente: Infografías ENS

RD 311/2022 – Revisión de medidas

Photo by You X Ventures on Unsplash

Aumentan considerablemente su nivel de exigencia (9)

- Identificación
- Configuración de seguridad
- Gestión de la configuración de seguridad
- Protección frente a código dañino
- Registro de actividad
- Gestión de la capacidad
- Detección de instrusión
- Sistema de métricas
- Aceptación y puesta en servicio

Aumentan ligeramente su nivel de exigencia (11)

- Requisitos de acceso
- Mantenimiento y actualizaciones de seguridad
- Gestión de cambios
- Gestión de incidentes
- Componentes certificados
- Deberes y obligaciones
- Protección de la configencialidad
- Separación de flujos de información en la red
- Borrado y destrucción
- Copias de seguridad
- Datos de caracter personal

Nuevas medidas (6)

- Servicios en la nube
- Interconexión de sistemas
- Protección de la cadena de suministros
- Medios alternativos
- Vigilancia
- Otros dispositivos conectados a la red

Se han eliminado (9)

- Protección de los registros de actividad.
- Personal alternativo
- Medios alternativos (4)
- Cifrado
- Instalaciones alternativas
- Accesp remoto

Se han simplificado (6)

- Segregación de tareas
- Protección de los dispositivos portátiles
- Perímetro seguro
- Sellos de tiempo
- Calificación de la información
- Protección frente a denegación de servicio

Fuente: Infografías ENS

RD 311/2022 – Requisitos y refuerzos codificados

✓**Codificación para facilitar** de manera proporcionada **la seguridad** de los sistemas de información, su **implantación** y su **auditoría.**

✓**Se han codificado los requisitos** de las medidas:

- **Requisitos base**
- Posibles **refuerzos de seguridad (R)**, alineados con el nivel de seguridad perseguido, que se suman (+) a los requisitos base de la medida.

  No siempre son incrementales entre sí; de forma que, en ciertos casos, se puede elegir entre aplicar un refuerzo u otro.

  Algunos refuerzos son de carácter opcional.

RD 311/2022 – Medidas de Seguridad Anexo II

Ej. Protección de servicios en la nube

sepian Seguridad Digital de Andalucía

4.5.1 Protección de servicios en la nube [op.nub.1].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	+ R1	+R1+R2

Requisitos.

– [op.nub.1.1] Los sistemas que suministran un servicio en la nube a organismos del sector público deberán cumplir con el conjunto de medidas de seguridad en función del modelo de servicio en la nube que presten: Software como Servicio (*Software as a Service, SaaS*), Plataforma como Servicio (*Platform as a Service, PaaS*) e Infraestructura como Servicio (*Infrastructure as a Service, IaaS*) definidas en las guías CCN-STIC que sean de aplicación.

– [op.nub.1.2] Cuando se utilicen servicios en la nube suministrados por terceros, los sistemas de información que los soportan deberán ser conformes con el ENS o cumplir con las medidas desarrolladas en una guía CCN-STIC que incluirá, entre otros, requisitos relativos a:

a) Auditoría de pruebas de penetración (*pentesting*).
b) Transparencia.
c) Cifrado y gestión de claves.
d) Jurisdicción de los datos.

Refuerzo R1- Servicios certificados.

– [op.nub.1.r1.1] Cuando se utilicen servicios en la nube suministrados por terceros, estos deberán estar certificados bajo una metodología de certificación reconocida por el Organismo de Certificación del Esquema Nacional de Evaluación y Certificación de Seguridad de las Tecnologías de la Información.

– [op.nub.1.r1.2] Si el servicio en la nube es un servicio de seguridad deberá cumplir con los requisitos establecidos en [op.pl.5].

Refuerzo R2-Guías de Configuración de Seguridad Específicas.

– [op.nub.1.r2.1] La configuración de seguridad de los sistemas que proporcionan estos servicios deberá realizarse según la correspondiente guía CCN-STIC de Configuración de Seguridad Específica, orientadas tanto al usuario como al proveedor.

Disposición transitoria única. Adecuación de sistemas.

1. Los sistemas de información del ámbito de aplicación del ENS, preexistentes a su entrada en vigor, dispondrán de veinticuatro meses para alcanzar su plena adecuación al ENS, circunstancia que se manifestará con la exhibición del correspondiente Distintivo de Conformidad, atendiendo lo dispuesto en el artículo 38 del ENS.

2. Los nuevos sistemas de información aplicarán lo establecido en el ENS desde su concepción.

Con el liderazgo de la Secretaría General de Administración Digital y el Centro Criptológico Nacional, junto con sus equipos de colaboradores, **el ENS es el resultado de un esfuerzo colectivo del sector público de España, con la colaboración del sector privado**, que vienen contribuyendo activamente a su elaboración, desarrollo, aplicación y evolución.

Photo by Annie Spratt on Unsplash

Qué se espera:


Photo by Paul Rysz on Unsplash

1. **Sector público → Partícipes y agentes de la ciberseguridad,** para llevarla a la realidad práctica.
2. **Sector privado → si trabaja para el sector público,** directa o indirectamente como **prestadores de servicios o proveedores de soluciones** (cadena de suministro), **colaboración para la plena aplicación del ENS.**

Identificación de Sistemas

Problemática en la identificación de sistemas.

- **Deficiente identificación**:
  - Excesiva atomización, o
  - Excesiva integración

- **NO ES son equivalentes** aplicación o servicio con sistema de información.

- Efectivamente: tener 30 aplicaciones diferentes en una misma Organización, dedicadas habitualmente a cooperar en el desenvolvimiento de una misma actividad administrativa NO SIGNIFICA NECESARIAMENTE tener 30 sistemas de información del ámbito de aplicación del ENS (con sus respectivas declaraciones de aplicabilidad, análisis de riesgos, etc.)

- La clave de la determinación efectiva de los sistemas de información está en la **segmentación efectiva de sistemas y redes**.

- Situación que se pretende evitar: que un incidente de seguridad que tiene su origen en un determinado sistema se traslade a otro sistema.

Categorización de Sistemas

sedian Seguridad Digital de Andalucía

Problemática en la categorización de sistemas.

- **Deficiente categorización**, una doble problemática:
  - Elevación innecesaria de requisitos, o
  - Relajación inadecuada o inconveniente de requisitos.

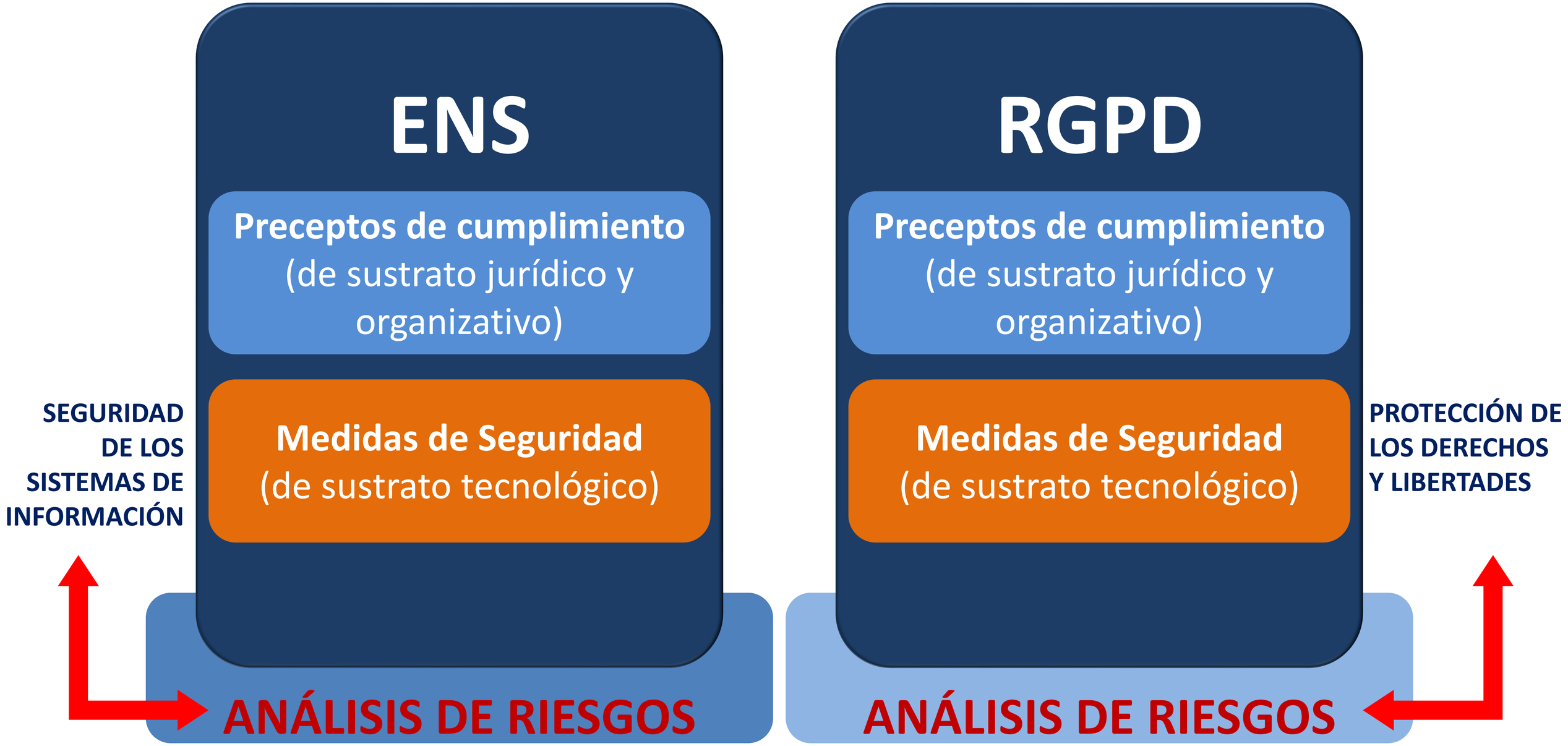
- La **categoría de seguridad** de un sistema de información vendrá determinada por:

  - El encuadramiento de la entidad en un determinado Perfil de Cumplimiento Específico, o
  - La seguridad exigible, derivada de los **riesgos para el sistema de información** de que se trate.
  - La seguridad exigible, derivada de los **riesgos para los derechos y libertades** de los titulares de los datos personales.
  - En ambos casos es necesario realizar un **análisis de riesgos**.

- No debe identificarse, necesariamente, tratamiento de categorías especiales de datos con sistemas de información de categoría Alta.

- Nada impide elevar el nivel de exigencia de una o varias medidas de seguridad, atendiendo a las especiales circunstancias que concurran en el caso (ejemplo).

Convergencia ENS ←→ RGPD



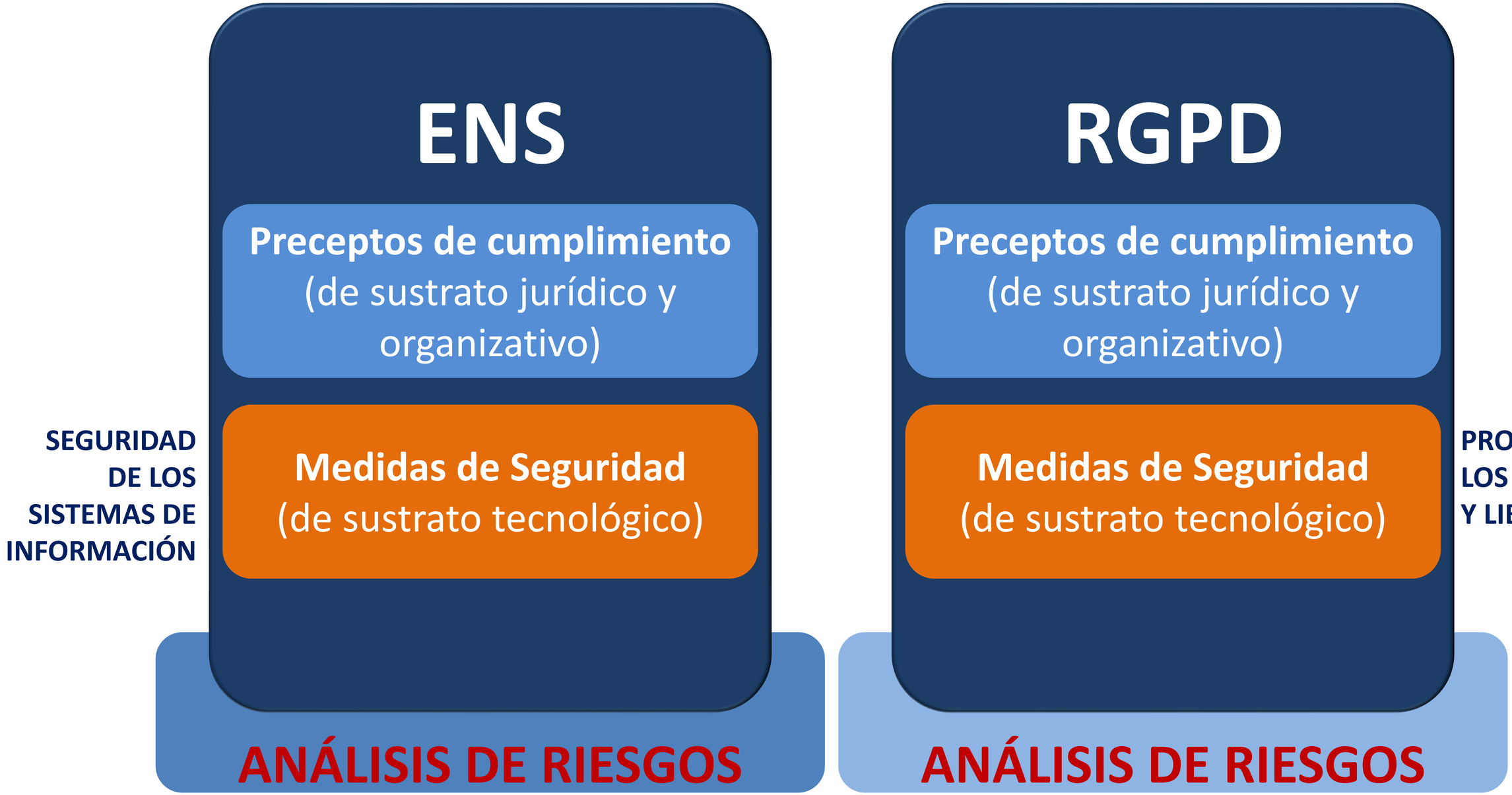
LEY ORGÁNICA 3/2018 DE PROTECCIÓN DE DATOS PERSONALES Y GARANTÍA DE LOS DERECHOS DIGITALES

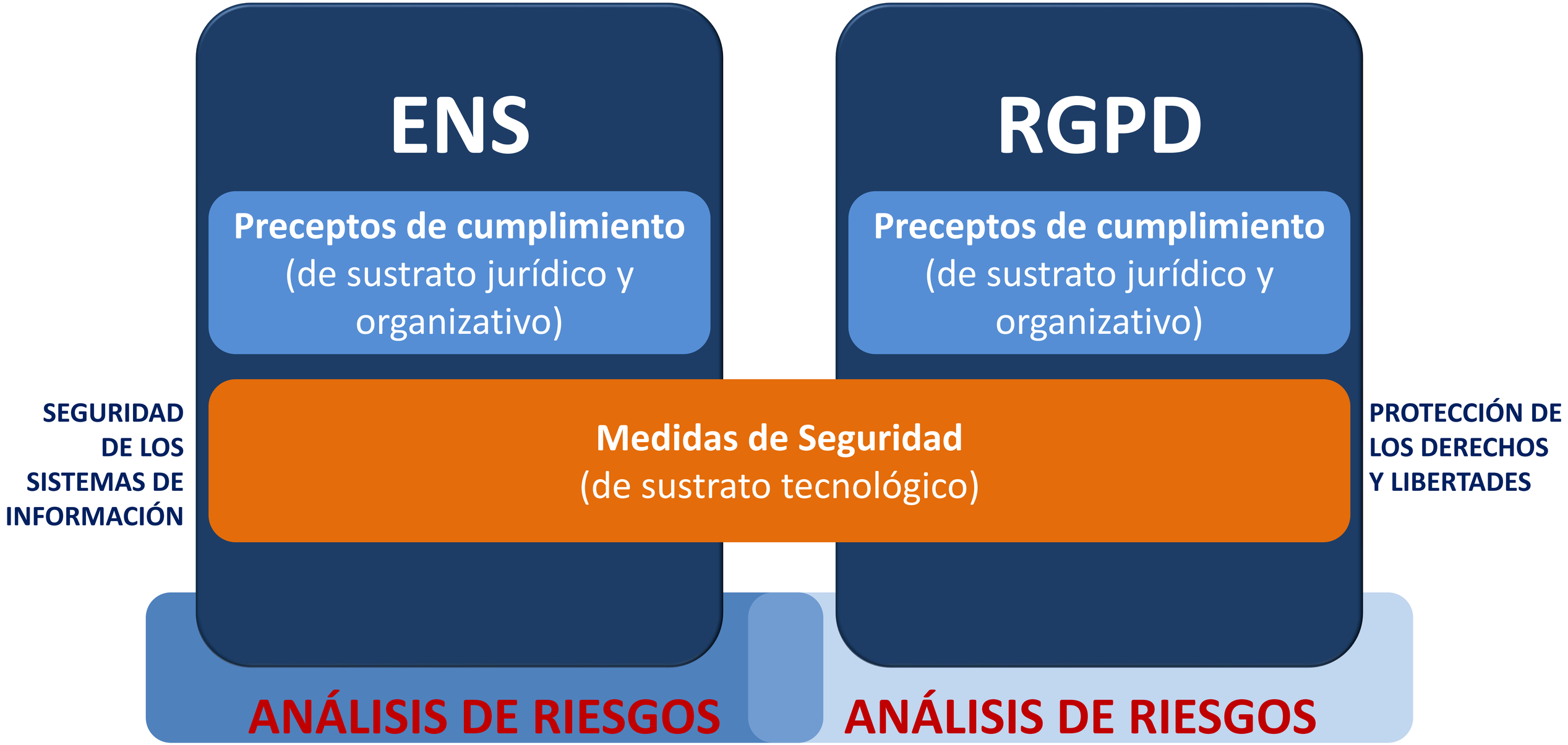
Disposición adicional primera. Medidas de seguridad en el ámbito del sector público.

1. **El Esquema Nacional de Seguridad incluirá las medidas que deban implantarse en caso de tratamiento de datos personales**, para evitar su pérdida, alteración o acceso no autorizado, adaptando los criterios de determinación del riesgo en el tratamiento de los datos a lo establecido en el artículo 32 del Reglamento (UE) 2016/679.

2. Los responsables enumerados en el artículo 77.1 de esta ley orgánica deberán **aplicar a los tratamientos de datos personales las medidas de seguridad que correspondan de las previstas en el Esquema Nacional de Seguridad**, así como impulsar un grado de implementación de medidas equivalentes en las empresas o fundaciones vinculadas a los mismos sujetas al Derecho privado.

En los casos en los que un tercero preste un **servicio en régimen de concesión, encomienda de gestión o contrato**, **las medidas de seguridad se corresponderán con las de la Administración pública de origen y se ajustarán al Esquema Nacional de Seguridad**.


ENS
Preceptos de cumplimiento
(de sustrato jurídico y organizativo)
Medidas de Seguridad
(de sustrato tecnológico)
SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN
ANÁLISIS DE RIESGOS
RGPD
Preceptos de cumplimiento
(de sustrato jurídico y organizativo)
Medidas de Seguridad
(de sustrato tecnológico)
PROTECCIÓN DE LOS DERECHOS Y LIBERTADES
ANÁLISIS DE RIESGOS


ENS
Preceptos de cumplimiento
(de sustrato jurídico y organizativo)
RGPD
Preceptos de cumplimiento
(de sustrato jurídico y organizativo)
SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN
Medidas de Seguridad
(de sustrato tecnológico)
PROTECCIÓN DE LOS DERECHOS Y LIBERTADES
ANÁLISIS DE RIESGOS
ANÁLISIS DE RIESGOS

La participación de terceros

- Hay que **determinar la asignación de responsabilidad de cada parte, proveedor y cliente**, respecto al articulado y, especialmente, a las medidas seguridad del Anexo II del ENS que sean de aplicación, según la categoría del sistema.

- Puede usarse la tabla en el Anexo I de la Guía CCN-STIC 858, que pueda servir de ejemplo de partida, dado que la casuística puede ser diversa.

- En la referida tabla se tiene en cuenta para cada una de las medidas de seguridad que determina el Anexo II del ENS:

  - El código y descripción de la medida.
  - La categoría del sistema para el que la medida es de aplicación.
  - El porcentaje de responsabilidad en la aplicación de la medida entre el proveedor que provisiona la solución y el cliente dónde se implanta.
  - Las acciones necesarias a ser llevadas a cabo por el proveedor.
  - Las acciones a ser llevadas a cabo por el cliente.
  - En determinados casos, notas de implantación.

- **El reparto de responsabilidades cliente-proveedor será fijado, en primera instancia, por el cliente, aunque podrá ser pactado por ambas partes, atendiendo a las especiales circunstancias que concurran en cada caso concreto.**

- El **Análisis de Riesgos** deberá ser realizado, conjuntamente, por el cliente y por el proveedor, asumiendo y responsabilizándose de sus resultados, en la parte que le corresponda a cada uno de ellos. Dicho Análisis de Riesgos será asimismo evaluado por la Entidad de Certificación, cuando el cliente se encuentre en un proceso de Auditoría de Certificación del ENS que involucre los sistemas de información sobre los que se prestan los servicios contratados o prestados.

ANEXO I (Ejemplo de asignación de responsabilidades entre proveedor y cliente)

Reparto de responsabilidades entre Proveedor y Cliente (Coordinación de aplicabilidad de medidas de seguridad del ENS)						
Medida de Seguridad	**Categoría**	**Responsabilidad**		**Acciones necesarias para el proveedor**	**Acciones necesarias para el cliente**	**Notas de implantación**
		Proveedor	**Cliente**			
org.1 Política de Seguridad	**TODAS**	50%	50%	El proveedor dispone de una política de seguridad accesible para el cliente, por ejemplo, en la URL: https://www.proveedor.es/politica-de-seguridad, o se le ha dado a conocer por otro medio.	Existirá una política de seguridad aprobada por el órgano superior.	La Política de Seguridad del Proveedor es necesaria solo hasta que el sistema se implanta en la infraestructura del cliente. A partir de ese momento, la única Política de Seguridad es la del cliente (que habrá de contemplar la presencia de sistemas *on-premise* y redactar preceptos en consecuencia).
org.2 Normativa de Seguridad	**TODAS**	50%	50%	En la Normativa Interna de uso de medios electrónicos en la organización, se incluirán capítulos o epígrafes específicos destinados a sistemas concretos. En este apartado, se incluirá la documentación necesaria para la implantación y el uso correcto de la solución para cumplir con el ENS. Los usuarios de la solución implantada disponen, por ejemplo, de un manual de usuario, paneles de ayuda, avisos desplegables, banners o mensajes emergentes, con normas de uso denotando sus responsabilidades.	Se dispondrá de normativa documentada relacionada con el uso correcto y con el inadecuado de los activos, junto a sus responsabilidades, derechos, deberes y medidas disciplinarias.	Los usuarios deben conocer las funciones de la solución implantada y, en su caso, aceptarán las condiciones de uso de la misma.
org.3 Procedimientos de seguridad	**TODAS**	50%	50%	Se encuentran documentadas las acciones necesarias para la instalación segura de la solución, los procedimientos de administración, así como instrucciones y protocolos de uso seguro de la solución por parte de sus usuarios.	Se adecuarán / complementarán los procedimientos de seguridad de todo el sistema de información para que contemplen la solución implantada.	
org.4 Procedimiento de autorización	**TODAS**	50%	50%	Se encuentra documentado el proceso de autorizaciones, correspondiente tanto a administradores como a usuarios, ya sea en el entorno de instalación (Guía de instalación), como en el entorno de operación (Guía de uso seguro / manual de usuario).	Existirá un proceso de autorizaciones adecuado a todo el sistema de información, que incluya la solución implantada.	

op.pl.1 Análisis de riesgos	**B**	**M**	**A**	Sí	Sí	El proveedor dispone de una gestión propia de riesgos en la que ha considerado los procesos de desarrollo, implantación, mantenimiento y soporte de la solución (en el caso de que se haya subcontratado). En la Guía de instalación segura que se facilita al cliente, el proveedor incluye un análisis de riesgos respecto a la solución que provee.	La organización cliente incluirá la solución implantada como activo o activos. La organización cliente dispondrá de un Análisis de Riesgos en el que incluirá los riesgos de gestionar soluciones ON-PREMISE y en su caso, cuando no se disponga de soporte del proveedor, deberán establecerse medidas en el plan de tratamiento de riesgos (PTR). Se incorporarán los riesgos identificados por el proveedor en la Guía de instalación de la solución en la gestión de riesgos global de la organización cliente.	Ambas partes (proveedor y cliente) deberán tener un análisis de riesgos actualizado.
op.pl.2 Arquitectura de seguridad	**B**	**M**	**A**	50%	50%	Se dispone de un mapa esquemático o diagrama con la arquitectura de la solución que se facilita en la Guía de instalación de la solución. Se contempla tanto a nivel de bloques de estructuración de los módulos software de la solución, como a nivel de arquitectura recomendada para implementar la misma (Balanceadores, servidores web, servidores de BBDD, etc.) e integrarla en la red del cliente. Se incluyen diagramas con indicación de las conexiones e interconexiones (flujos de datos) hacia otros sistemas y hacia el exterior, con indicación de cómo se han protegido, o pueden protegerse, incluyendo los protocolos de acceso empleados. Se documentarán en la Guía de instalación las recomendaciones de configuración y parametrización para mantener un nivel adecuado de seguridad.	La organización cliente dispondrá de documentación de las instalaciones, del sistema, de accesos al sistema, de la(s) red(es), de las líneas de defensa... de modo que se facilite la integración de la solución contratada.	
op.pl.3 Adquisición de nuevos componentes	**TODAS**			50%	50%	Cuando se incorporen o sustituyan elementos que afecten al desarrollo de software, como módulos o librerías, el proveedor de la solución verifica que no rompe la seguridad. Si es necesario establece acciones de formación y sensibilización.	La organización cliente dispondrá de un proceso para planificar las adquisiciones de soluciones que considere los riesgos, los elementos existentes en la arquitectura actual del sistema y las necesidades que pueden surgir de su integración.	
op.pl.4 Dimensionamiento / Gestión de la Capacidad	**B**	**M**	**A**	50%	50%	Se le entregan a la organización cliente de la solución ON-PREMISE, en la Guía de instalación, tablas para poder dimensionar los recursos que la soportarán, en función del nº de usuarios, nº de trámites y de otros parámetros que se estimen relevantes. Se dimensiona en base a	La organización cliente dispondrá de un estudio con la evolución histórica de la capacidad del sistema, o Plan de Capacidad, que permita dimensionar los componentes en los que se apoyará la solución con ayuda de las tablas proporcionadas por el fabricante en la Guía de	La información de la solución se almacena en Base de Datos, siendo responsabilidad del cliente que contrata definir los umbrales de almacenamiento en su sistema y programar las alertas adecuadas cuando se alcancen dichos umbrales.

					recursos de procesador, memoria, capacidad en disco, recursos humanos, etc. Asimismo, la solución contempla parametrizar y elaborar estadísticas, permitiendo la monitorización del almacenamiento y gestionar la retención de la información.	instalación.	
op.pl.5 Componentes certificados	**B**	**M**	**A**	100%	0%	Para categoría alta, los componentes adicionales, proporcionados conjuntamente con la solución implantada, están certificados.	La organización cliente procurará que los componentes de la infraestructura TIC que interactúen con la solución implantada estén certificados.	
op.acc.1 Identificación	**TODAS**			70%	30%	La solución cubre las necesidades del cliente facilitándole la gestión de los usuarios: Identificación, estado, responsable o área a la que pertenece, roles asignados, permisos en base a dichos roles, etc.	Se procedimentará a nivel interno la gestión de los usuarios registrados en sus sistemas. El cliente deberá gestionar mediante procedimientos las altas, modificaciones y bajas de usuarios, así como las autorizaciones y notificaciones de dichos cambios.	La solución implantada dispone de mecanismos de consulta para listar los usuarios dados de alta en la aplicación. Los usuarios de la solución implantada pueden ser dados de baja o deshabilitados en cualquier momento y pueden tener definida una fecha de caducidad previamente establecida.
op.acc.2 Requisitos de acceso	**TODAS**			50%	50%	La solución no permite que un usuario sin estar dado de alta, o sin los oportunos permisos, pueda acceder a recursos no habilitados.	La organización cliente gestionara los derechos de acceso de todo el sistema, incluidos los derechos de acceso que puedan corresponder a los usuarios a la solución implantada.	
op.acc.3 Segregación de funciones y tareas	**B**	**M**	**A**	70%	30%	La solución implantada permite la segregación de funciones y tareas mediante la asignación de permisos a usuarios específicos y a grupos de usuarios. La solución implantada permite la gestión diferenciada de las tareas críticas por dos o más usuarios mediante flujos, restringiendo los accesos individuales. Se pueden lanzar notificaciones o alertas a un usuario Administrador. La solución considera la separación de funciones de operación, configuración, mantenimiento y auditoria; no permite accesos a entornos o capas no asociadas a un perfil de acceso.	Existirá un proceso interno documentado, relacionado con la segregación de funciones y tareas en el sistema de información de la organización cliente.	En la solución implantada se pueden definir los distintos usuarios y grupos de usuarios. Se gestiona la asignación de permisos mediante opciones de menú, asociación de roles a los usuarios o grupos, etc., lo que permite establecer a qué funcionalidades accede cada usuario. La solución dispone de opciones de consulta y listado de usuarios y grupos, junto a las funcionalidades permitidas.
Op.acc.4 Proceso de gestión de derechos de acceso	**TODAS**			30%	70%	La aplicación permite la asignación y el bloqueo o cancelación ágiles de accesos de usuario.	La organización cliente dispondrá de un proceso interno relacionado con las altas, modificaciones y bajas de los usuarios, asociado con los principios de mínima funcionalidad, necesidad de conocer y capacidad de autorizar (según la medida de seguridad org.4).	

Roles y Responsabilidades

Premisas

- CCN-STIC-801 establece unas pautas de carácter general, aplicables a entidades de distinta naturaleza y dimensión.
- Cada organización tendrá que adaptarla a su propia situación.

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

RD 311/2022 – Esquema Nacional de Seguridad:

4

Artículo 11. *Diferenciación de responsabilidades.*

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

2. **La responsabilidad de la seguridad de los sistemas de información estará diferenciada de la responsabilidad sobre la explotación de los sistemas de información concernidos *[Resp. Sistema].***

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

Artículo 13. *Organización e implantación del proceso de seguridad.*

1. La seguridad de los sistemas de información deberá comprometer a todos los miembros de la organización.

2. La política de seguridad, en aplicación del principio de diferenciación de responsabilidades a que se refiere el artículo 11 y según se detalla en la sección 3.1 del anexo II, deberá ser conocida por todas las personas que formen parte de la organización e identificar de forma inequívoca a los responsables de velar por su cumplimiento, los cuales tendrán las siguientes funciones:

a) El **responsable de la información** determinará los requisitos de la información tratada
b) El **responsable del servicio** determinará los requisitos de los servicios prestados.
c) El **responsable de la seguridad** determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios, supervisará la implantación de las medidas necesarias para garantizar que se satisfacen los requisitos y reportará sobre estas cuestiones.
d) El **responsable del sistema**, por sí o a través de recursos propios o contratados, se encargará de desarrollar la forma concreta de implementar la seguridad en el sistema y de la supervisión de la operación diaria del mismo, pudiendo delegar en administradores u operadores bajo su responsabilidad.
…

…
3. El responsable de la seguridad será distinto del responsable del sistema, no debiendo existir dependencia jerárquica entre ambos. En aquellas situaciones excepcionales en las que la ausencia justificada de recursos haga necesario que ambas funciones recaigan en la misma persona o en distintas personas entre las que exista relación jerárquica, deberán aplicarse medidas compensatorias para garantizar la finalidad del principio de diferenciación de responsabilidades previsto en el artículo 11.

4. Una Instrucción Técnica de Seguridad regulará el Esquema de Certificación de Responsables de la Seguridad, que recogerá las condiciones y requisitos exigibles a esta figura.

5. En el caso de servicios externalizados, salvo por causa justificada y documentada, la organización prestataria* de dichos servicios deberá designar un POC (Punto o Persona de Contacto) para la seguridad de la información tratada y el servicio prestado, que cuente con el apoyo de los órganos de dirección, y que canalice y supervise, tanto el cumplimiento de los requisitos de seguridad del servicio que presta o solución que provea, como las comunicaciones relativas a la seguridad de la información y la gestión de los incidentes para el ámbito de dicho servicio.
Dicho POC de seguridad será el propio Responsable de Seguridad de la organización contratada, formará parte de su área o tendrá comunicación directa con la misma. Todo ello sin perjuicio de que la responsabilidad última resida en la entidad del sector público destinataria de los citados servicios.

* Debe decir: *prestadora*

(*) Errata: debe decir *prestadora*

Objeto de la Guía CCN-STIC-801

MARCO DE REFERENCIA

que

- Establezca las **responsabilidades** generales en la gestión de la Seguridad IT.
- Proponer **roles de seguridad** que asuman dichas responsabilidades.

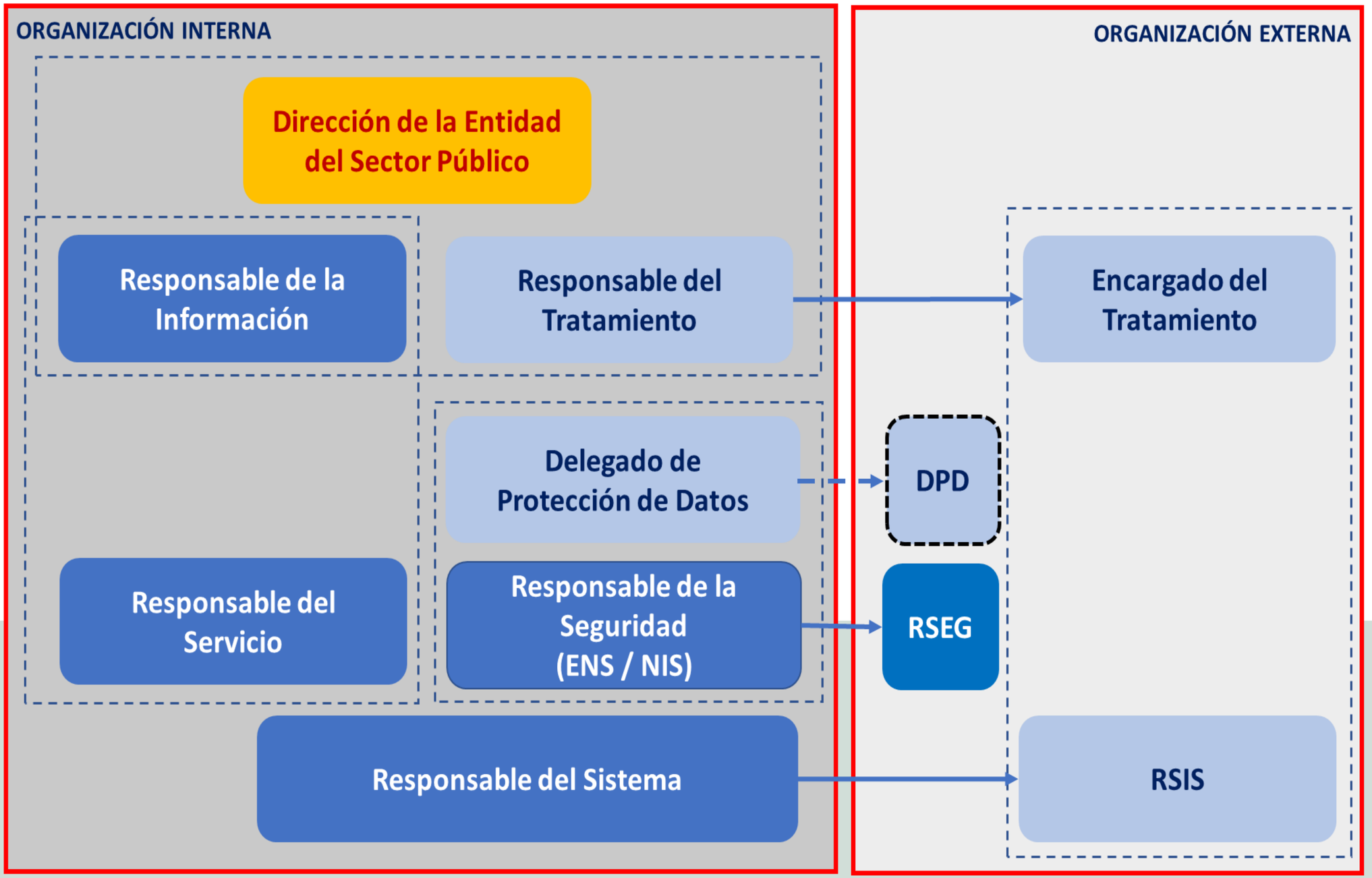
Es responsabilidad de cada organismo establecer su propia
Organización de Seguridad, de acuerdo con sus necesidades y características

- La estructura propuesta en la Guía CCN-STIC-801 sirve como guía.

- La implantación final puede ser diferente en cada organización.

- Importante → Las responsabilidades definidas en la Guía deben ser cubiertas sea cual fuere la solución final adoptada.

Estructura Propuesta en la Guía CCN-STIC-801:

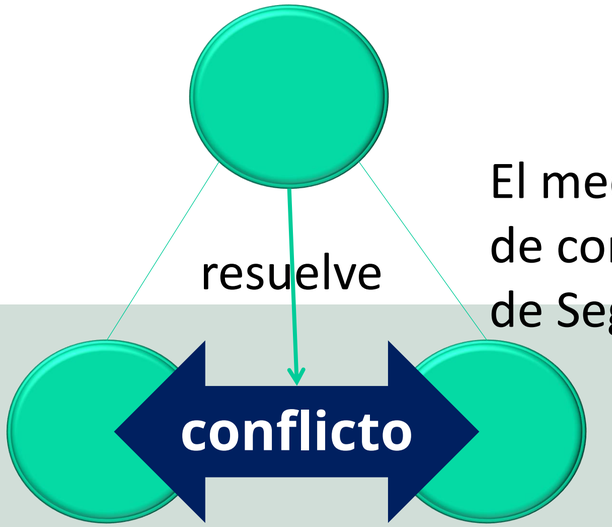


Bloques de responsabilidad

Niveles de la estructura de seguridad

Segregación

Resolución de Conflictos



El mecanismo concreto de resolución de conflictos debe figurar en la Política de Seguridad del Organismo.

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.

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.

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.

RESPONSABLE DE LA INFORMACIÓN
(information owner)

Origen de la información

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.

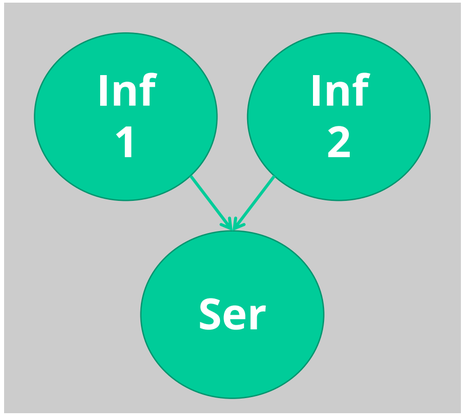
- La determinación de **los niveles de seguridad** en cada dimensión de seguridad debe realizarse dentro del marco establecido en el **Anexo I** del Esquema Nacional de Seguridad.
- Se recomienda **que los criterios de valoración estén respaldados por la Política de Seguridad** en la medida en que sean 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.

¿RESPONSABLE DE LA INFORMACIÓN = RESPONSABLE DEL SERVICIO?

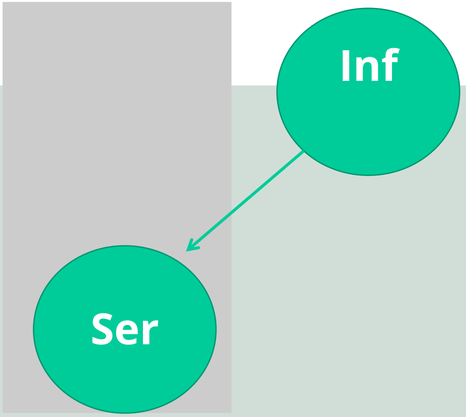
Es posible que coincidan en la misma persona u órgano las responsabilidades de la información y del servicio.

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**



RESPONSABLE DE LA INFORMACIÓN + RESPONSABLE DEL SERVICIO

Como quiera que de la valoración realizada por ambos responsables (de la Información y de los Servicios) se derivará la categoría de seguridad de los sistemas de información en cuestión y, en su consecuencia, las medidas de seguridad a adoptar (que podrán ser más o menos rigurosas u onerosas en función de esta categorización), **la determinación final de tales valoraciones por parte de una única entidad es muy frecuente en determinadas instituciones (como es el caso de las entidades prestadoras de servicios públicos o administrativos), puesto que permite que una figura de alto rango administrativo o gerencial de la entidad (por ejemplo, el Consejero Delegado, Director General, Secretario General, etc.), sobradamente conocedor de las informaciones tratadas por la entidad y los servicios prestados, sea el que, partiendo de evaluaciones previas realizadas por elementos concretos de la organización, se encuentre en las mejores condiciones para valorar adecuada y uniformemente la información tratada y los servicios prestados (desde los puntos de vista de las dimensiones de seguridad del ENS: disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad), lo que redundará en una mejor determinación de la categoría de seguridad del sistema y, en consecuencia, las medidas de seguridad a implantar.**

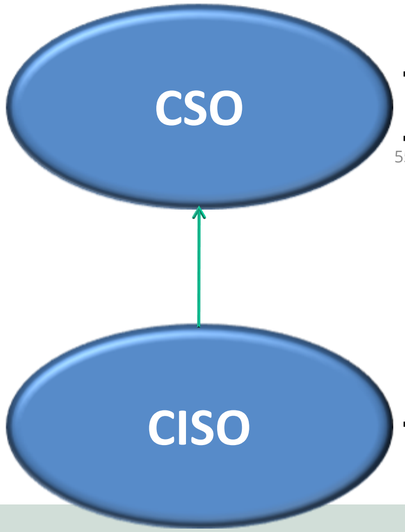
RESPONSABLE DE LA SEGURIDAD

- 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.

- Otras denominaciones:
  - NIST: *Computer Security Program Manager [SP 800-12]*
  - NIST: *Chief Information Security Officer [SP 800-53]*
  - Unión Europea: Autoridad INFOSEC (ASTIC) [2001/264/CE]
  - CCN: Autoridad de Seguridad de las Tecnologías de la Información y Comunicación (ASTIC) [CCN-STIC 201]
  - Ministerio de Defensa: Autoridad INFOSEC (AI) [OM 76/2002]

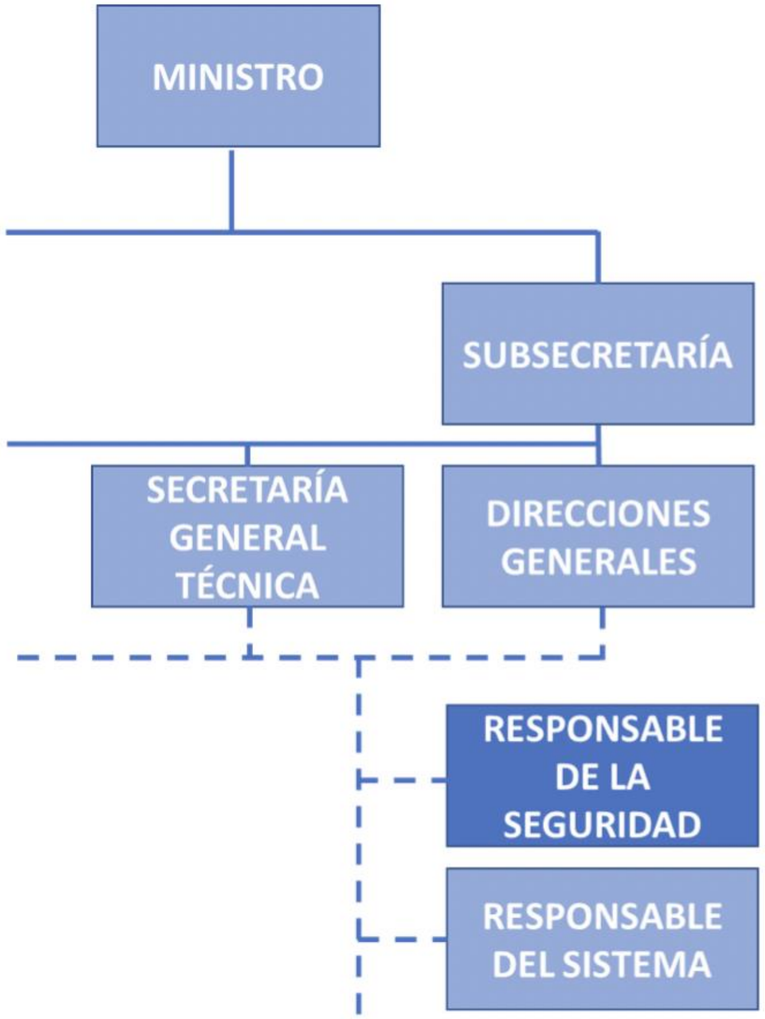
RESPONSABLE DE LA SEGURIDAD



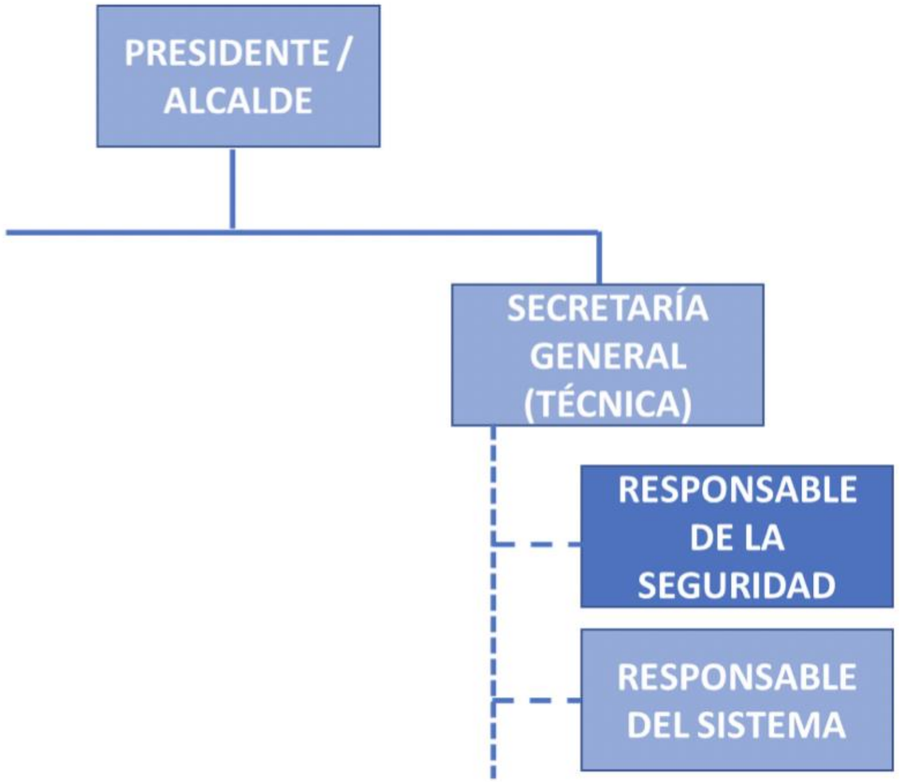
→ Visión de negocio
→ Responsable de Seguridad Corporativa

→ Centrado en la Seguridad IT

RESPONSABLE DE LA SEGURIDAD

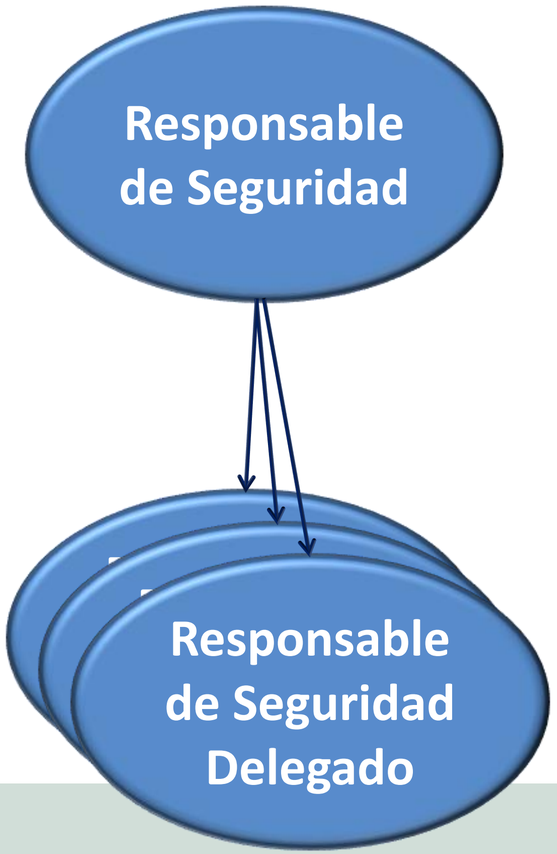


AGE, Departamento Ministerial (tipo)



Entidad Local (tipo)

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 Resp. Seg. 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.

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.

SEGURIDAD FÍSICA

- Cuando la seguridad física (de las instalaciones) esté segregada de la seguridad lógica, esta se ajustará a lo establecido por el ENS en materia de seguridad física.

- El Responsable de la Seguridad Física implantará las medidas de seguridad que le competan dentro de las determinadas por el Responsable de la Seguridad de la Información, e informará a éste de su grado de implantación, eficacia e incidentes.

GESTIÓN DEL PERSONAL

- Los responsables de RRHH se ajustarán a lo establecido por el ENS en materia de personal.

- Los responsables de RRHH implantarán las medidas de seguridad que les competan dentro de las determinadas por el Responsable de Seguridad de la Información, e informarán a éste de su grado de implantación, eficacia e incidentes.

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.

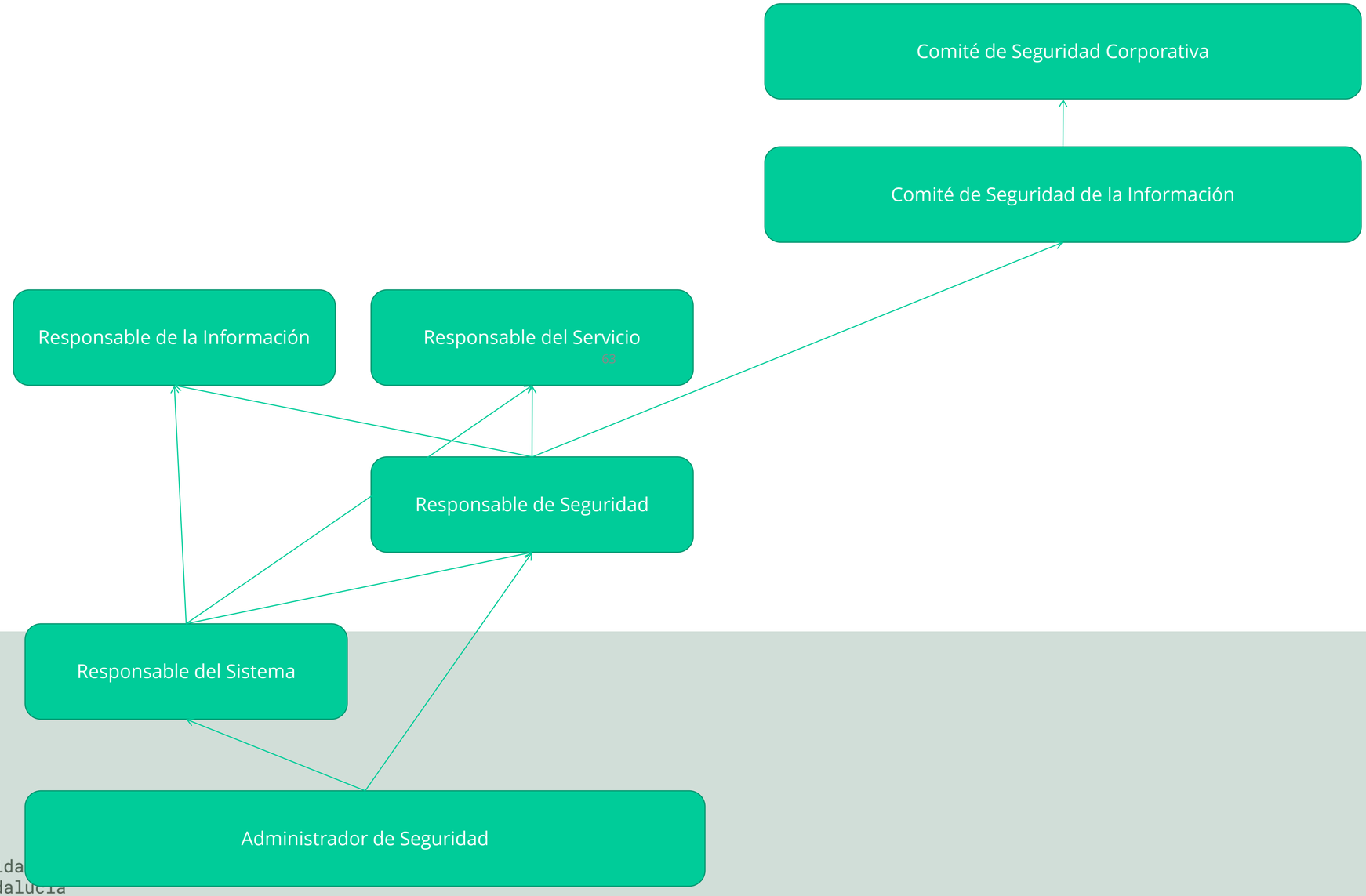
- Algunas responsabilidades pueden instrumentarse por medio de Comités, que se articularán y funcionarán como órganos colegiados de acuerdo con la normativa administrativa.

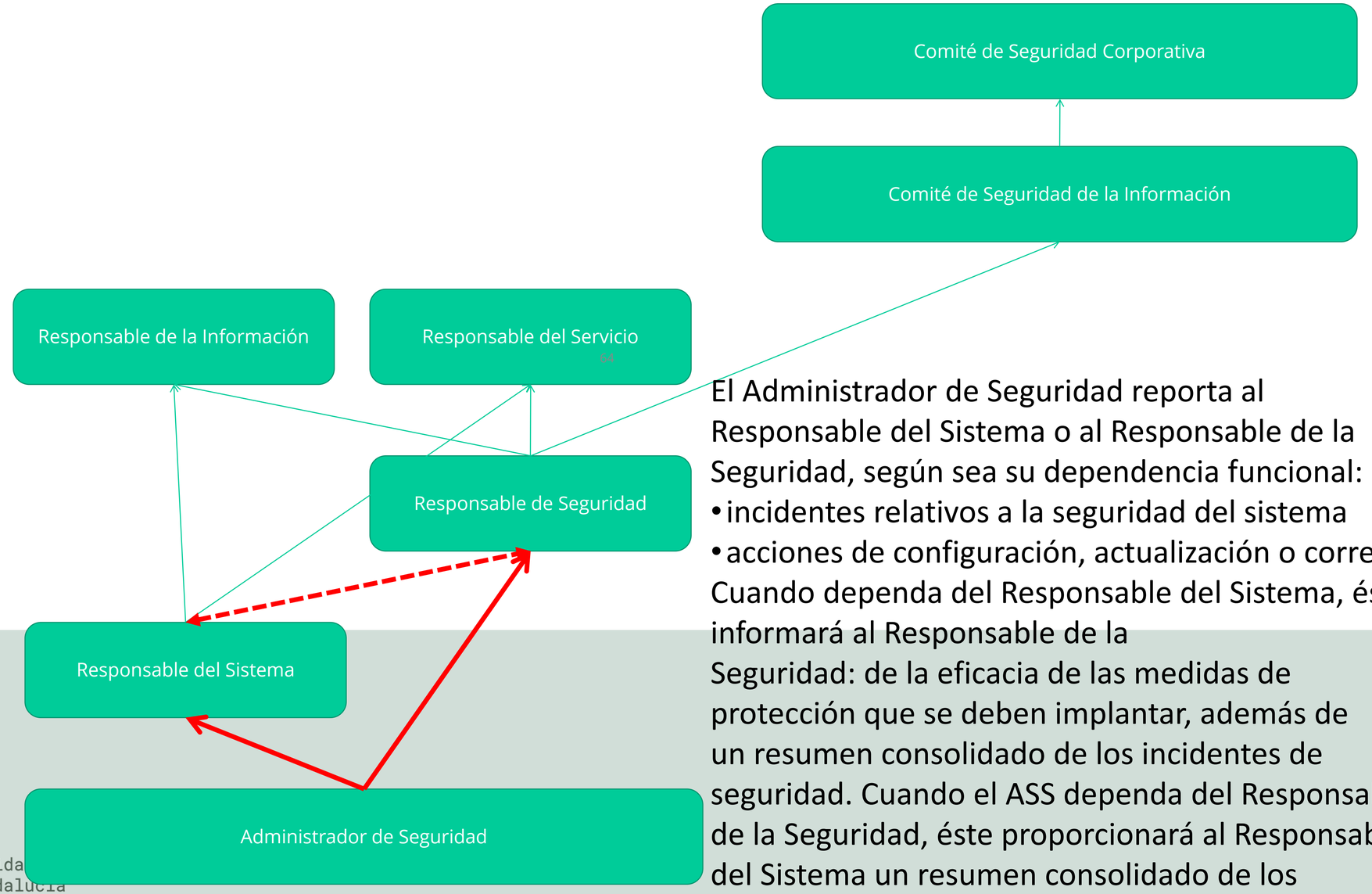
- Son habituales los siguientes:

  - **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.

Ejemplo: un modelo para una entidad prestadora de servicios públicos

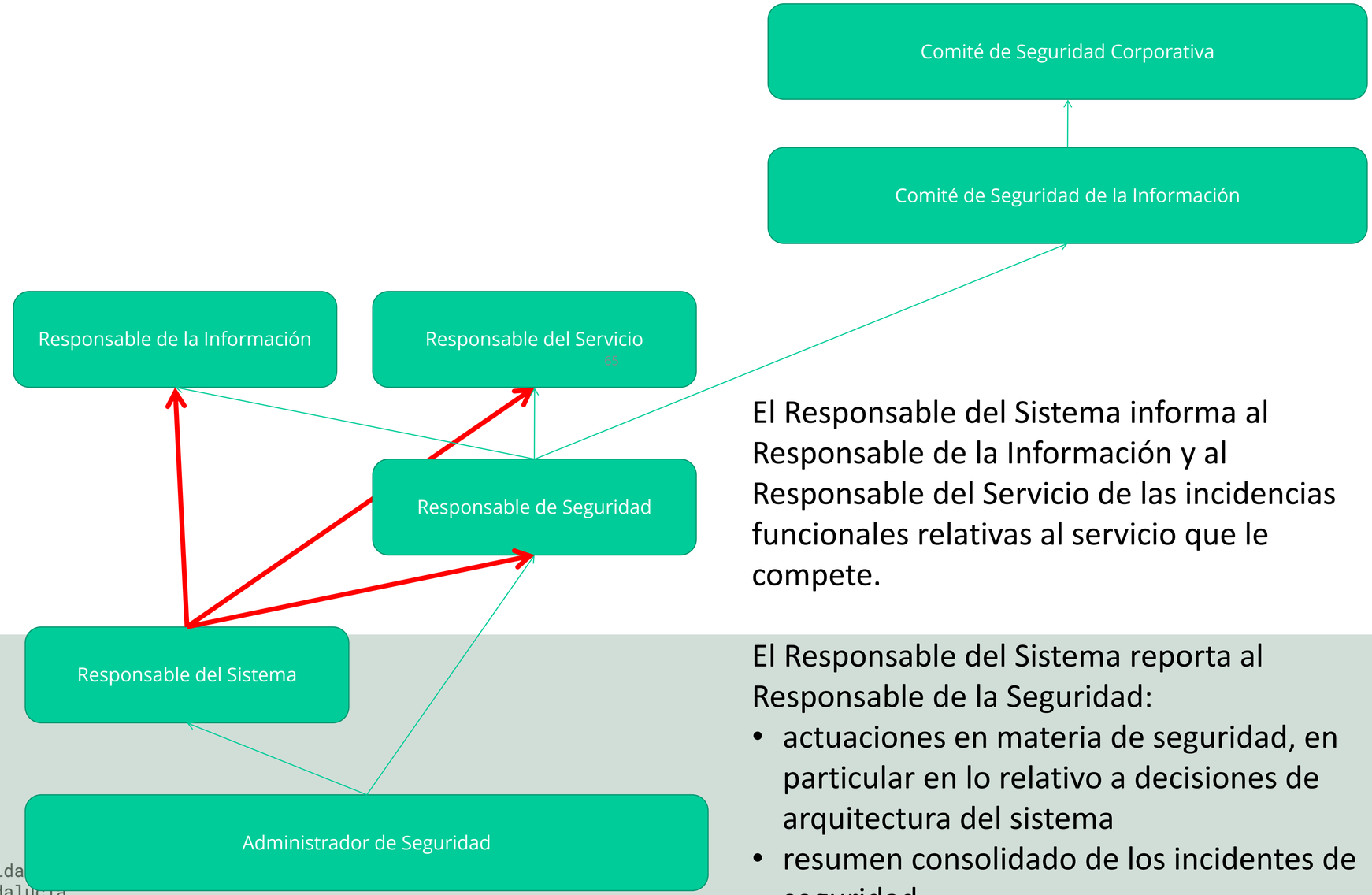

Comité de Seguridad Corporativa
Comité de Seguridad de la Información
Responsable de la Información
Responsable del Servicio
Responsable de Seguridad
Responsable del Sistema
Administrador de Seguridad



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 correc.

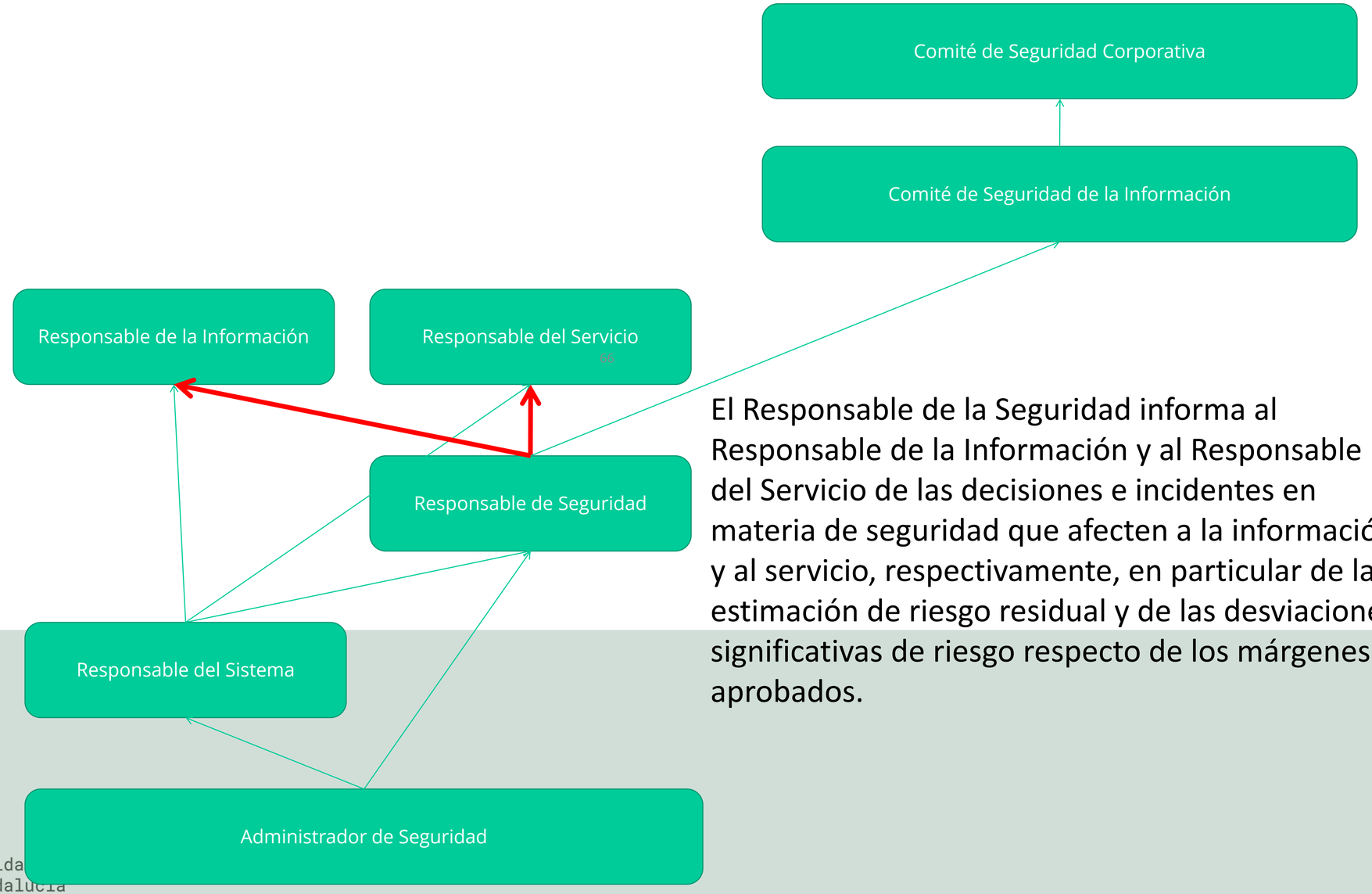
Cuando dependa del Responsable del Sistema, éste informará al Responsable de la Seguridad: de la eficacia de las medidas de protección que se deben implantar, además de un resumen consolidado de los incidentes de seguridad. Cuando el ASS dependa del Responsable de la Seguridad, éste proporcionará al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



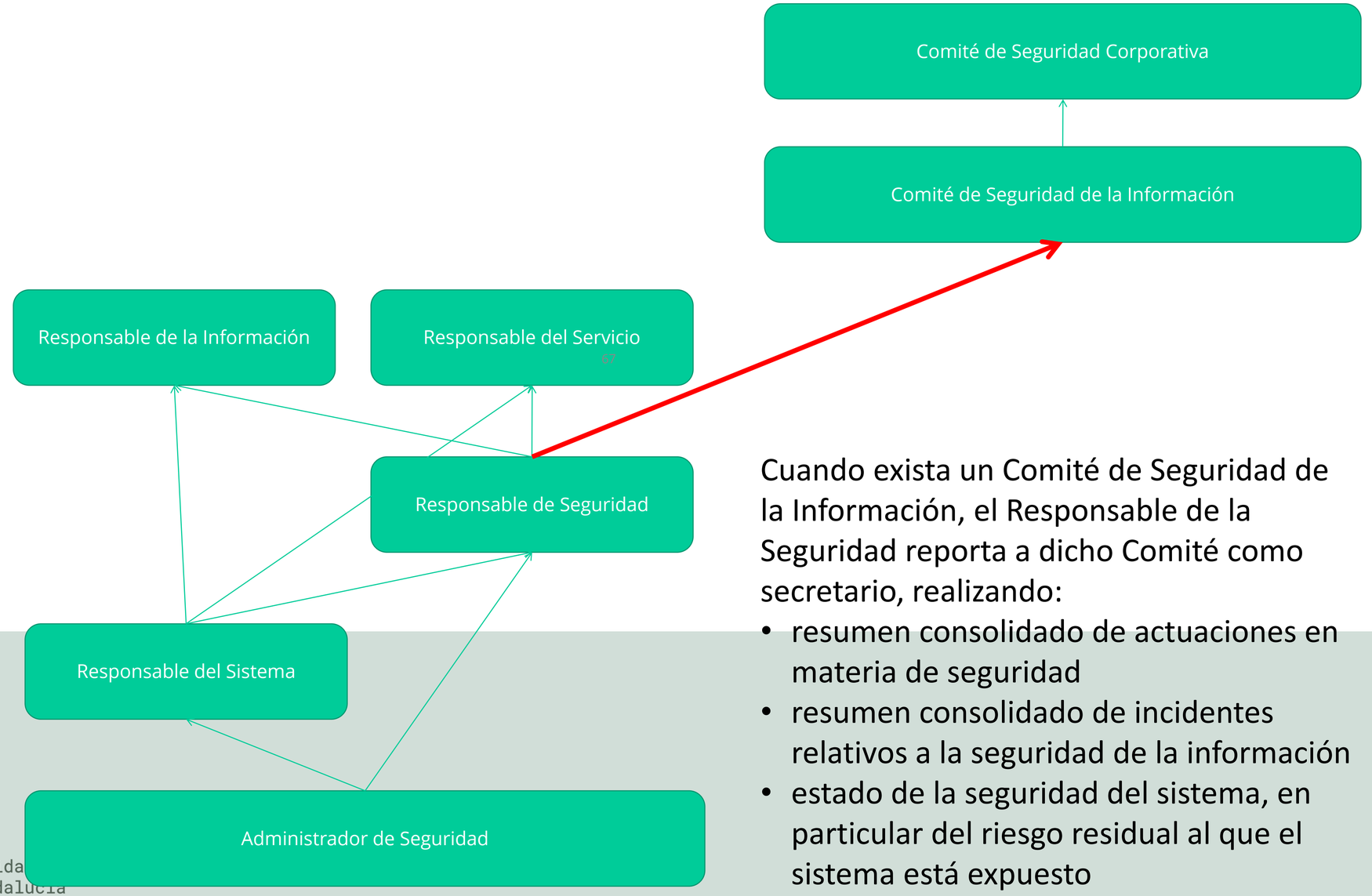
El Responsable del Sistema informa al Responsable de la Información y al Responsable del Servicio de las incidencias funcionales relativas al servicio que le compete.

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
- resumen consolidado de los incidentes de seguridad

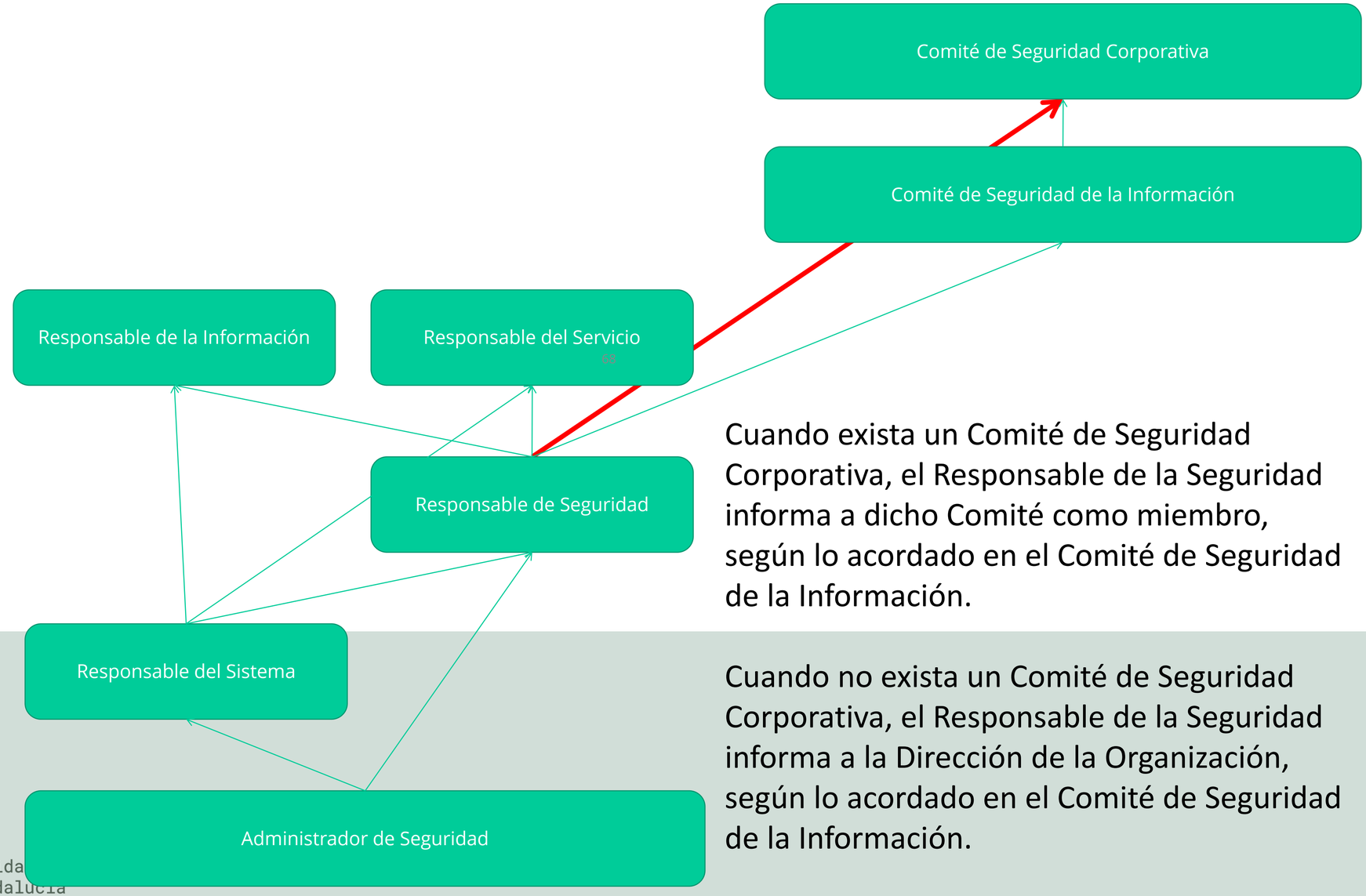


El Responsable de la Seguridad informa al Responsable de la Información y al Responsable del Servicio de las decisiones e incidentes en materia de seguridad que afecten a la información y al servicio, respectivamente, en particular de la estimación de riesgo residual y de las desviaciones significativas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



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.

	Rol	Descripción
A	**Accountable**	**Toma la decisión** (y responde de ello). A veces se dice que **Autoriza** (el trabajo a realizar) y **Aprueba** (el trabajo finalizado y, a partir de ese momento, se hace responsable de él). Sólo puede existir un A por cada tarea. Se trata de la figura que debe asegurar que se ejecutan las tareas.
R	**Responsible**	**Realiza el trabajo** (previamente autorizado por A) y es responsable por su realización. Lo habitual es que exista un solo R. Si existe más de uno, entonces el trabajo debería ser subdividido a un nivel más bajo. Se trata de la figura que debe ejecutar las tareas.
C	**Consulted**	**Se le consulta antes de tomar la decisión**. Este rol posee alguna información o capacidad necesaria para terminar el trabajo. Se le informa y se le consulta información (comunicación bidireccional).
I	**Informed**	**Se le informa de las decisiones tomadas.** Este rol debe ser informado sobre el progreso y los resultados del trabajo. A diferencia del Consultado, la comunicación es unidireccional.

Tarea	Dirección	RINFO	RSERV	RSEG	RSIS	AS
niveles de seguridad requeridos por la información		A	I	R	C	
niveles de seguridad requeridos por el servicio		I	A	R	C	
determinación de la categoría del sistema		I	I	R	I	
análisis de riesgos	A	I	I	R	C	
declaración de aplicabilidad		I	I	A/R	C	
medidas de seguridad adicionales		I	I	A/R	C	
configuración de seguridad		I	I	A	C	R
aceptación del riesgo residual	A	C	C	R	I	
documentación de seguridad				A	C	I
política de seguridad	A	C	C	R	C	
normativa de seguridad		C	C	A	C	I
procedimientos de seguridad		I	I	C	A	I
implantación de las medidas de seguridad		I	I	C	A	R
supervisión de las medidas de seguridad				A	I	R
estado de seguridad del sistema	I	I	I	A	I	R
planes de mejora de la seguridad		I	I	A/R	C	
planes de concienciación y formación		I	I	A	C	
planes de continuidad		I	I	C	A	
suspensión cautelar del servicio	I	I	I	A	R	
seguridad en el ciclo de vida				C	A	

Muchas gracias

cgalan@atl.es
cgalan@der-pu.uc3m.es

ENS: ens@ccn-cert.cni.es

sedian Seguridad Digital de Andalucía