

Guía de Seguridad de las TIC CCN-STIC 801

ESQUEMA NACIONAL DE SEGURIDAD RESPONSABILIDADES Y FUNCIONES



MARZO 2019

Edita:



© Editor y Centro Criptológico Nacional, 2019

NIPO: 083-19-158-4

Fecha de Edición: Marzo, 2019

Los Sres. Carlos Galán y José Antonio Mañas han participado en la redacción del documento.

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

Quedan rigurosamente prohibidas, sin la autorización escrita del **Centro Criptológico Nacional**, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos.

PRÓLOGO

El uso masivo de las tecnologías de la información y las telecomunicaciones (TIC), en todos los ámbitos de la sociedad, ha creado un nuevo espacio, el ciberespacio, donde se producirán conflictos y agresiones, y donde existen ciberamenazas que atentarán contra la seguridad nacional, el estado de derecho, la prosperidad económica, el estado de bienestar y el normal funcionamiento de la sociedad y de las administraciones públicas.

La Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia (CNI), encomienda al Centro Nacional de Inteligencia el ejercicio de las funciones relativas a la seguridad de las tecnologías de la información en su artículo 4.e), y de protección de la información clasificada en su artículo 4.f), a la vez que confiere a su Secretario de Estado Director la responsabilidad de dirigir el Centro Criptológico Nacional (CCN) en su artículo 9.2.f).

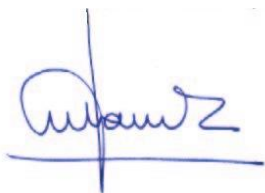
Partiendo del conocimiento y la experiencia del CNI sobre amenazas y vulnerabilidades en materia de riesgos emergentes, el Centro realiza, a través de su Centro Criptológico Nacional, regulado por el Real Decreto 421/2004, de 12 de marzo, diversas actividades directamente relacionadas con la seguridad de las TIC, orientadas a la formación de personal experto, a la aplicación de políticas y procedimientos de seguridad, y al empleo de tecnologías de seguridad adecuadas.

El 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 (ENS, en adelante), al que se refiere el apartado segundo del artículo 156 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, establece la política de seguridad en la utilización de medios electrónicos que permita una protección adecuada de la información.

Precisamente el Real Decreto 3/2010 de 8 de Enero, actualizado por el Real Decreto 951/2015, de 23 de octubre, fija los principios básicos y requisitos mínimos así como las medidas de protección a implantar en los sistemas de la Administración, y promueve la elaboración y difusión de guías de seguridad de las tecnologías de la información y las comunicaciones (STIC) por parte de CCN para facilitar un mejor cumplimiento de dichos requisitos mínimos.

En definitiva, la serie de documentos CCN-STIC se elabora para dar cumplimiento a los cometidos del Centro Criptológico Nacional y a lo reflejado en el Esquema Nacional de Seguridad, conscientes de la importancia que tiene el establecimiento de un marco de referencia en esta materia que sirva de apoyo para que el personal de la Administración lleve a cabo su difícil, y en ocasiones, ingrata tarea de proporcionar seguridad a los sistemas de las TIC bajo su responsabilidad.

Marzo de 2019



Félix Sanz Roldán
Secretario de Estado
Director del Centro Criptológico Nacional

ÍNDICE

| | |
|---|-----------|
| 1. OBJETO DE LA GUÍA..... | 4 |
| 2. ACTORES Y RESPONSABLES | 4 |
| 3. ESTRUCTURA DE LA SEGURIDAD | 9 |
| 4. RESOLUCIÓN DE CONFLICTOS | 13 |
| 5. NIVEL DE GOBIERNO: LOS RESPONSABLES DE LA INFORMACIÓN Y DEL SERVICIO..... | 13 |
| 5.1. EL RESPONSABLE DE LA INFORMACIÓN | 13 |
| 5.2. EL RESPONSABLE DEL SERVICIO..... | 14 |
| 5.3. RESPONSABILIDADES UNIFICADAS | 15 |
| 6. NIVEL DE SUPERVISIÓN: EL RESPONSABLE DE LA SEGURIDAD | 15 |
| 7. NIVEL OPERATIVO: EL RESPONSABLE DEL SISTEMA | 18 |
| 7.1. EL RESPONSABLE DEL SISTEMA..... | 18 |
| 7.2. SEGURIDAD FÍSICA..... | 19 |
| 7.3. GESTIÓN DEL PERSONAL | 19 |
| 8. EL ADMINISTRADOR DE SEGURIDAD (AS)..... | 19 |
| 9. COMITÉS..... | 21 |
| 9.1. COMITÉ DE SEGURIDAD CORPORATIVA | 22 |
| 9.2. COMITÉ DE SEGURIDAD DE LA INFORMACIÓN | 23 |
| 10. NOMBRAMIENTOS | 25 |
| 11. REPORTES Y FLUJO DE INFORMACIÓN | 25 |
| 12. GESTIÓN DE LOS RIESGOS..... | 27 |
| 13. CONCURRENCIA CON EL RGPD | 30 |
| ANEXO A. RESPUESTA A INCIDENTES Y MATRIZ RACI..... | 32 |
| ANEXO B. ESTRUCTURAS POSIBLES DE IMPLANTACIÓN | 35 |

1. OBJETO DE LA GUÍA.

Esta guía establece unas pautas de carácter general que son aplicables a todas las entidades del sector público sin entrar en casuísticas particulares. En consecuencia, se espera que cada organización las particularice para adaptarlas a su naturaleza, competencias y entorno singular.

1. El objeto de esta guía es proponer un marco de referencia que establezca las responsabilidades generales en la gestión de la seguridad de los sistemas de información de las entidades del Sector Público del ámbito subjetivo de aplicación del RD 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de seguridad (ENS), desarrollando las figuras o roles más significativos que asuman dichas responsabilidades.
2. Tomando como base las directrices señaladas en esta guía, cada entidad debe establecer y aprobar su propia Organización de Seguridad, de acuerdo con su naturaleza, estructura, dimensión y recursos disponibles, que deberá estar recogida en la Política de Seguridad de la Información de la entidad y, cuando se traten datos de carácter personal, en la Política de Protección de Datos.

2. ACTORES Y RESPONSABLES

3. La gestión de la seguridad de los sistemas de información en las organizaciones -definición, implantación y mantenimiento- exige establecer una **Organización de la Seguridad**. Tal organización debe determinar con precisión los diferentes actores que la conforman, sus funciones y responsabilidades, así como la implantación de una estructura que las soporte.
4. El artículo 10 del ENS señala (las negritas son nuestras):

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.

5. Además de las tres figuras mencionadas en el art. 10 del ENS -**Responsable de la Información, Responsable del Servicio y Responsable de la Seguridad**-, cuyas competencias y responsabilidades pueden ser indelegables¹, las organizaciones suelen

¹ Parece claro que, mientras que las responsabilidades del Responsable de la Información y Responsable del Servicio son siempre indelegables, no ocurre lo mismo con las correspondientes al Responsable de la Seguridad, que podrían ser asumidas, como competencias propias, por las Diputaciones Provinciales, en el caso de las entidades locales. Por tanto, habrá que sostener, con carácter general, que todas las responsabilidades mencionadas son indelegables en tanto no exista una habilitación legal que permita la delegación.

- disponer también del denominado **Responsable del Sistema** (de información²), y cuya responsabilidad puede estar situada dentro de la organización (utilización de sistemas propios) o estar compartimentada entre una **responsabilidad mediata**³ (de la propia organización) y una **responsabilidad inmediata** (de terceros, públicos o privados), cuando los sistemas de información se encuentran externalizados⁴.
6. Por otro lado, cuando la entidad está tratando datos de carácter personal, se hace necesario contemplar las figuras de **Responsable del Tratamiento**, **Delegado de Protección de Datos** y, en su caso, **Encargado del Tratamiento**, con las funciones definidas en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (RGPD, en adelante); y en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD, en adelante).
 7. El cuadro siguiente muestra las peculiaridades de las figuras más significativas en materia de seguridad de la información, atendiendo a la norma legal de la que traen causa.

| Entidad | Ubicación legal | Funciones, Características o Referencias |
|---|--|---|
| Dirección de la Entidad del Sector Público | La derivada de la aplicación de la Ley 40/2015 | Entidades del Sector Público del ámbito de aplicación del ENS, cuyo titular ostenta la máxima responsabilidad en el desarrollo de las competencias de la entidad, incluyendo las de seguridad de la información, de conformidad con lo dispuesto en la Ley 40/2015 y en el resto del ordenamiento jurídico. Es el máximo responsable de la implantación del ENS. |
| Responsable de la Información | ENS, art. 10 | Determina los requisitos (de seguridad) de la información tratada, según los parámetros del Anexo I del ENS. Puede tratarse de una persona física singular o un órgano colegiado, formando parte de lo que se suele denominar Comité de Seguridad de la Información. Como la seguridad constituye un principio de actuación propio de las entidades públicas, la aprobación de los niveles de seguridad de la |

² El ENS define “sistema de información” como: “Conjunto organizado de recursos para que la información se pueda recoger, almacenar, procesar o tratar, mantener, usar, compartir, distribuir, poner a disposición, presentar o transmitir”. (Anexo IV. Glosario).

³ Es “autor mediato” quien causa un resultado sirviéndose de otra persona como medio o instrumento para realizar la ejecución. El autor no realiza directa y personalmente el delito, se sirve de otra persona consciente de la trascendencia penal que tiene su acto.

⁴ Cuando se utilizan servicios externalizados (mediante contrato, convenio, encomienda, etc.), es frecuente que la entidad prestadora (pública o privada) cuente asimismo con un Responsable de la Seguridad al que será exigible el mantenimiento de la seguridad de los sistemas de información concernidos, sin que ello suponga merma de la responsabilidad exigible al Responsable de la Seguridad de la entidad pública destinataria de los servicios.

| Entidad | Ubicación legal | Funciones, Características o Referencias |
|------------------------------------|-----------------|--|
| | | información constituye asimismo una actividad indelegable. |
| | ENS, art. 43 | La valoración de las consecuencias de un impacto negativo sobre la seguridad de la información se efectuará atendiendo a su repercusión en la capacidad de la organización para el logro de sus objetivos, la protección de sus activos, el cumplimiento de sus obligaciones de servicio, el respeto de la legalidad y los derechos de los ciudadanos. |
| Responsable del Servicio | ENS, art. 10 | <p>Determina los requisitos (de seguridad) de los servicios prestados, según los parámetros del Anexo I del ENS.</p> <p>Puede tratarse de una persona física singular o un órgano colegiado, formando parte de lo que se suele denominar Comité de Seguridad de la Información.</p> <p>Como la seguridad constituye un principio de actuación propio de las entidades públicas, la aprobación de los niveles de seguridad de los servicios constituye asimismo una actividad indelegable.</p> |
| | ENS, art. 39 | Debe incluir las especificaciones de seguridad en el ciclo de vida de los servicios y sistemas, acompañadas de los correspondientes procedimientos de control. |
| | ENS, art. 43 | Valorará las consecuencias de un impacto negativo sobre la seguridad de los servicios se efectuará atendiendo a su repercusión en la capacidad de la organización para el logro de sus objetivos, la protección de sus activos, el cumplimiento de sus obligaciones de servicio, el respeto de la legalidad y los derechos de los ciudadanos. |
| Responsable de la Seguridad | ENS, art. 10 | <p>Determina las decisiones de seguridad pertinentes para satisfacer los requisitos establecidos por los responsables de la información y de los servicios.</p> <p>Deberá ser una persona física, jerárquicamente independiente del Responsable del Sistema.</p> <p>Nota: En caso de servicios externalizados, la responsabilidad última la tiene siempre la entidad del Sector Público destinataria de los servicios, aun cuando la responsabilidad inmediata pueda corresponder (vía contrato,</p> |

| Entidad | Ubicación legal | Funciones, Características o Referencias |
|---------|------------------------------|--|
| | | convenio, encomienda, etc.) a la organización prestataria del servicio. |
| | ENS, art. 15.3 | Las Administraciones públicas exigirán, de manera objetiva y no discriminatoria, que las organizaciones que les presten servicios de seguridad cuenten con profesionales cualificados y con unos niveles idóneos de gestión y madurez en los servicios prestados. |
| | ENS, art 18 | En la adquisición de productos de seguridad de las tecnologías de la información y comunicaciones se utilizarán, de forma proporcionada a la categoría del sistema y nivel de seguridad determinados, aquellos que tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición, salvo en aquellos casos en que las exigencias de proporcionalidad en cuanto a los riesgos asumidos no lo justifiquen a juicio del Responsable de la Seguridad. |
| | ENS, arts. 27.3, 27.4 y 27.5 | <p>Las medidas del Anexo II del ENS, así como aquellas otras necesarias para garantizar el adecuado tratamiento de datos personales podrán ser ampliadas por causa de la concurrencia indicada o del prudente arbitrio del Responsable de la Seguridad del sistema, habida cuenta del estado de la tecnología, la naturaleza de los servicios prestados y la información manejada, y los riesgos a que están expuestos.</p> <p>La relación de medidas seleccionadas del Anexo II se formalizará en un documento denominado Declaración de Aplicabilidad, firmado por el Responsable de la Seguridad.</p> <p>Las medidas de seguridad referenciadas en el Anexo II podrán ser reemplazadas por otras compensatorias siempre y cuando se justifique documentalmente que protegen igual o mejor el riesgo sobre los activos (Anexo I) y se satisfacen los principios básicos y los requisitos mínimos previstos en los capítulos II y III del real decreto. Como parte integral de la Declaración de Aplicabilidad se indicará de forma detallada la correspondencia entre las medidas compensatorias implantadas y las medidas del Anexo II que compensan y el conjunto será objeto de la aprobación formal por parte del responsable de la seguridad.</p> |

| Entidad | Ubicación legal | Funciones, Características o Referencias |
|--|---|--|
| | ENS, art. 28 | La utilización de infraestructuras y servicios comunes reconocidos en las Administraciones Públicas facilitará el cumplimiento de los principios básicos y los requisitos mínimos exigidos en el ENS en condiciones de mejor eficiencia. Los supuestos concretos de utilización de estas infraestructuras y servicios comunes serán determinados por cada Administración. |
| | ENS, art. 34.6 y Anexo III | Los informes de autoevaluación y/o los informes de auditoría serán analizados por el Responsable de la Seguridad competente, que elevará las conclusiones al Responsable del Sistema para que adopte las medidas correctoras adecuadas. |
| Entidad Responsable de la Seguridad de la Información | Propuesta de Reglamento de Desarrollo del RD-I 12/2018 ⁵ | Véase epígrafe 6. |
| Responsable del Sistema (de información) | ENS | Se encarga de la operación del sistema de información, atendiendo a las medidas de seguridad determinadas por el Responsable de la Seguridad. |
| | La derivada de la aplicación de la Ley 40/2015 | Su responsabilidad puede estar situada dentro de la organización (utilización de sistemas propios) o estar compartimentada entre una responsabilidad mediata (de la propia organización) y una responsabilidad inmediata (de terceros, públicos o privados), cuando los sistemas de información se encuentran externalizados. |
| | ENS, art. 34.6 y 34.7 | Los informes de autoevaluación y/o los informes de auditoría serán analizados por el Responsable de la Seguridad competente, que elevará las conclusiones al Responsable del Sistema para que adopte las medidas correctoras adecuadas. En el caso de los sistemas de categoría ALTA, visto el dictamen de auditoría, el responsable del sistema podrá acordar la retirada de operación de alguna información, de algún servicio o del sistema en su totalidad, durante el tiempo que |

⁵ Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información. En el momento de redactar estas líneas, este RD-I está siendo tramitado como Proyecto de Ley, al tiempo que se está redactando su Reglamento de Desarrollo, que recogerá definitivamente las funciones y competencias de esta Entidad Responsable de la Seguridad de la Información. Por tanto, la lista de funciones indicada no debe considerarse definitiva.

| Entidad | Ubicación legal | Funciones, Características o Referencias |
|--|--|---|
| | | estime prudente y hasta la satisfacción de las modificaciones prescritas. |
| Responsable del Tratamiento (Protección de Datos) | RGPD, art. 4.7) y LOPDGDD, Título V | La persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros. |
| Encargado del Tratamiento (Protección de Datos) | RGPD, art. 4.8) y LOPDGDD, Título V | La persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del Responsable del Tratamiento. |
| Delegado de Protección de Datos | RGPD, art. 39 y LOPDGDD, arts. 34 a 37 | Ver epígrafe 13. |

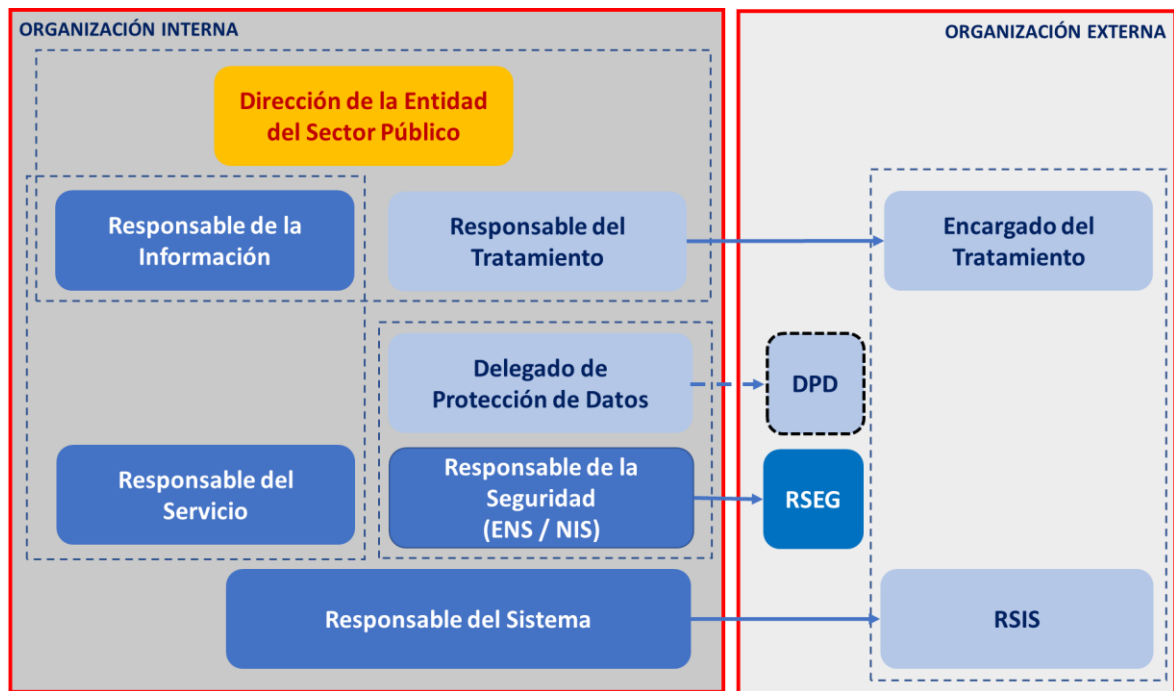
9. Más adelante se incluyen algunas precisiones adicionales en torno a estas figuras.
10. Como quiera que ciertas entidades del Sector Público también estarían comprendidas en el alcance del Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información⁶, se ha incluido en el cuadro anterior una primera lista de funciones del Responsable de la Seguridad de la Información, figura enunciada en el art. 16.3 de dicho cuerpo legal, y cuyas definitivas competencias y características se regularán en el preceptivo desarrollo reglamentario⁷.

3. ESTRUCTURA DE LA SEGURIDAD

11. Atendiendo a lo señalado en los epígrafes precedentes, podemos representar la Estructura de Seguridad (de la Información y de Protección de Datos) según se muestra en la figura siguiente.

⁶ Que transpone al ordenamiento jurídico español la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión (conocida como Directiva NIS).

⁷ Desarrollo reglamentario en fase de redacción en el momento de escribir estas líneas.



Esquema conceptual de la Seguridad de la Información y la Protección de Datos

12. La figura anterior representa un Esquema conceptual de la estructura de Seguridad de la Información y la Protección de Datos, señalando la ubicación o posibles ubicaciones de las figuras que se mencionan, independientemente de su posición concreta en la entidad pública de que se trate o la existencia de posibles Comités u órganos colegiados en los que pudiera integrarse algunas de tales figuras.
13. En base a la figura anterior, podemos señalar lo siguiente:
 1. La operativa de una entidad del Sector Público del ámbito de aplicación del ENS y del RGPD puede requerir el concurso de terceros externos a la propia organización (públicos o privados). Por este motivo, en la figura aparecen los roles correspondientes a la organización interna y también aquellos otros que pudieran ubicarse en organizaciones externas.
 2. Por imperativo legal, la responsabilidad máxima -también en materia de seguridad de la información ENS y protección de datos- se encuentra en el Titular (Dirección) de la entidad del Sector Público (o del titular del centro directivo) de que se trate, que, generalmente, personificará la figura del Responsable del Tratamiento del RGPD.
 3. Las figuras de Responsable de la Información y Responsable del Servicio pueden recaer en la misma persona, Comité u órgano colegiado. Dependiendo de la naturaleza o tamaño de la organización, ambas figuras podrán ser coincidentes asimismo con la del Titular de la entidad del Sector Público de que se trate.
 4. El Responsable de la Seguridad de la entidad pública poseerá una responsabilidad inmediata. No obstante, si se utilizan o contratan servicios de terceros (públicos o privados, como sería el caso de Servicios en la Nube) es imperativo que tales terceros cuenten asimismo con un Responsable de la Seguridad. En este caso, el Responsable de la Seguridad de la entidad pública poseerá una responsabilidad mediata, tal y como hemos señalado en el epígrafe 2 anterior.

5. Cuando se contratan con terceros determinadas actividades que comporten el tratamiento de datos personales, el Encargado del Tratamiento⁸, en la parte que le corresponda, podrá asumir eventualmente la figura de Responsable del Sistema (con una responsabilidad inmediata sobre el mismo).

El Delegado de Protección de Datos (DPD) puede ser interno o externo a la organización, pudiendo revestir asimismo la forma de un órgano colegiado (Comité Delegado de Protección de Datos), velando siempre por evitar conflicto de intereses en cualquiera de sus miembros. Además de ello, podrá designarse un único DPD para varias autoridades u organismos públicos, teniendo en consideración su estructura y tamaño.

6. La AEPD ha señalado la posibilidad de que el Delegado de Protección de Datos coincida con el Responsable de la Seguridad del ENS *“en aquellas organizaciones que, por su tamaño y recursos, no pudieran observar dicha separación, sería admisible la designación como delegado de protección de datos de la persona que ejerciera las funciones de responsable de seguridad del ENS, siempre que en la misma concurren los requisitos de formación y capacitación previstos en el RGPD. Además, resultaría imprescindible adoptar todas las medidas organizativas, debidamente reflejadas en su Política de seguridad de la información, que garantice la necesaria independencia y la ausencia de conflicto de intereses, por lo que no podría recibir instrucciones respecto al desempeño de sus funciones como delegado de protección de datos, deberá responder directamente al más alto nivel jerárquico y no podrá participar en las decisiones relativas a los fines y medios del tratamiento. En todo caso, esta circunstancia, que como decíamos, tiene carácter excepcional, deberá evaluarse caso por caso, y deberá dejarse documentada dicha designación haciendo constar los motivos por lo que el organismo correspondiente no ha podido observar dicha separación de funciones así como las medidas que garantizan la necesaria independencia del delegado de protección de datos⁹.”*
7. De conformidad con el principio de “segregación de funciones y tareas” recogido en el art. 10 del ENS, el Responsable de la Seguridad será una figura diferenciada del Responsable del Sistema.

14. El Esquema propuesto diferencia tres grandes bloques de responsabilidad:

1. La **responsabilidad legal** y la **especificación de las necesidades o requisitos**, que corresponde a la Dirección de la entidad y a los responsables del tratamiento, de la información y del servicio,
2. La **supervisión**, que corresponde al Responsable de la Seguridad y al Delegado de Protección de Datos, en sus respectivos ámbitos.
3. La **operación del sistema** de información, que corresponde al Responsable del Sistema.

15. La figura siguiente muestra estos bloques de responsabilidad:

⁸ El Encargado del Tratamiento, además de un tercero, puede ser una unidad de carácter interno a la propia organización, incluso con NIF diferenciado, prestando servicios a la entidad de la que depende a tales efectos.

⁹ AEPD: Informe 2018-0170: Incompatibilidad entre DPD y Responsable de la Seguridad.



Bloques de responsabilidad

16. Como hemos señalado, es posible -y habitual, en organizaciones de tamaño significativo- la existencia de ciertos órganos o comités que pueden colaborar en la seguridad de la entidad, ya sea física, de la información, de protección de datos, o todas ellas.
17. Los más habituales de tales comités son:
- Comité de Seguridad Corporativa.
 - Comité de Seguridad de la Información y
 - Comité de Protección de Datos¹⁰.
18. La figura siguiente muestra el encaje habitual de estos comités en una estructura establecida en tres **niveles**: gobierno, ejecutivo/supervisión y operacional.



Niveles de la estructura de seguridad

19. Cuando haya órganos colegiados, estos se constituirán de conformidad con lo dispuesto en la Sección 3ª del Capítulo II de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

¹⁰ Cuando, excepcionalmente, pudiera constituirse un Comité conjunto Seguridad de la Información – Protección de Datos, se deberá tener especial cuidado en analizar los posibles conflictos de intereses, muy especialmente en lo que se refiere al Delegado de Protección de Datos, que, en el ejercicio de sus funciones, no podrá recibir instrucciones, debiendo responder directamente al más alto nivel jerárquico y no podrá participar en las decisiones relativas a los fines y medios del tratamiento. La Política de Seguridad de la organización y los Términos de Referencia de este Comité deberán reflejar claramente las cautelas adoptadas en tal sentido, conforme a lo dispuesto en el precitado Informe Jurídico de la AEPD 2018-0170. Por otro lado, cuando se constituyan Comités separados, nada obsta para que, teniendo en cuenta las precisiones señaladas, algunos miembros de ambos comités sean coincidentes, como sucede habitualmente con las Oficinas o Unidades de apoyo a la Seguridad de la Información.

4. RESOLUCIÓN DE CONFLICTOS

20. De conformidad con lo dispuesto en el artículo 3 de la Ley 40/2015, que señala que las Administraciones Públicas, sirviendo los intereses generales, desarrollarán su actividad con plena observancia de los principios de eficacia, jerarquía, descentralización, desconcentración y coordinación, los conflictos entre distintos elementos de la organización serán resueltos por el superior jerárquico.
21. El mecanismo concreto de resolución de controversias debe figurar en la Política de Seguridad de la Información de la organización.
22. Seguidamente, se examinan los roles correspondientes a los tres niveles señalados.

5. NIVEL DE GOBIERNO: LOS RESPONSABLES DE LA INFORMACIÓN Y DEL SERVICIO.

23. La responsabilidad de la actividad de una entidad del sector Público se sitúa, en última instancia, en su Titular.
24. Mientras que las competencias o funciones de una entidad deben estar recogidas en su norma de creación o en las sucesivas normas de desarrollo de su estructura, el Titular de la Entidad es responsable de fijar los objetivos estratégicos, organizar adecuadamente sus elementos constituyentes, sus relaciones internas y externas, y dirigir su actividad, incluyendo la aprobación de la Política de Seguridad de la Información del organismo, así como, en su caso, la Política de Protección de Datos, facilitando los recursos adecuados para alcanzar los objetivos propuestos, velando por su cumplimiento.
25. Así pues, la figura de la Dirección de la entidad (personificada en su Titular) cobra una importancia capital: de la Dirección depende el compromiso de la entidad con la seguridad y su adecuada implantación, gestión y mantenimiento.
26. Por otro lado, suele ser habitual que en una entidad del Sector Público coexistan diferentes informaciones y servicios. La Política de Seguridad de la Información (y Protección de Datos, en su caso) deberá identificar claramente a quién corresponden las funciones que se han señalado con anterioridad para el Responsable de la Información, del Servicio, de Seguridad, del Sistema y Delegado de Protección de Datos, pudiendo determinar, además, aquellos puestos que serían incompatibles para el desempeño de estas funciones.
27. Con las salvedades señaladas con anterioridad, es posible que una misma persona pueda aunar varias responsabilidades o formar éstas parte de un órgano colegiado.

5.1. EL RESPONSABLE DE LA INFORMACIÓN

28. La información es la materia prima de la que se nutre la actividad de las entidades del Sector Público y puede tener su origen en la propia entidad, los ciudadanos y en terceras entidades (públicas o privadas).



Origen de la información

29. El Responsable de la Información¹¹ es habitualmente una persona situada en el nivel Directivo de la organización. Esta figura tiene la responsabilidad última del uso que se haga de una cierta información y, por tanto, de su protección. El Responsable de la Información es el responsable último de cualquier error o negligencia que conlleve un incidente de confidencialidad o de integridad (en materia de protección de datos) y de disponibilidad (en materia de seguridad de la información).
30. Como hemos visto en el primer epígrafe de esta Guía, el ENS asigna al Responsable de la Información la potestad de establecer los requisitos de la información en materia de seguridad. O, en terminología del ENS, la potestad de determinar los niveles de seguridad de la información, pudiendo ser una persona física concreta o un órgano colegiado.
31. Aunque la aprobación formal de los niveles corresponda al Responsable de la Información, se puede recabar una propuesta al Responsable de la Seguridad y conviene que se escuche la opinión del Responsable del Sistema¹².
32. La determinación de los niveles 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.

5.2. EL RESPONSABLE DEL SERVICIO

33. El ENS asigna al Responsable del Servicio la potestad de establecer los requisitos del servicio en materia de seguridad. O, en terminología del ENS, la potestad de determinar los niveles de seguridad de los servicios, pudiendo ser una persona física concreta o un órgano colegiado, como hemos visto con anterioridad.
34. 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 Sistema¹³.

¹¹ Information Owner: Official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, classification, collection, processing, dissemination, and disposal. See also information steward.

NIST 800-53: Official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal. [CNSSI_4009:2010]

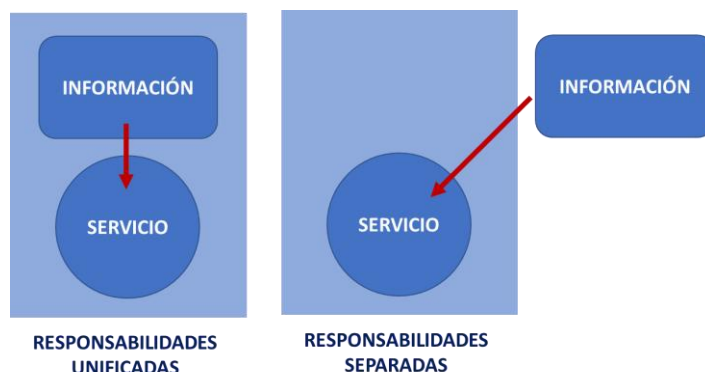
¹² Naturalmente, la responsabilidad última de la adecuada determinación del nivel de seguridad de la información tratada (y los riesgos asumibles) se encuentra en el Titular de la entidad del Sector Público de que se trate, figura que, como hemos visto, puede ser coincidente con la del Responsable de la Información.

¹³ Naturalmente, la responsabilidad última de la adecuada determinación del nivel de seguridad del servicio prestado (y los riesgos asumibles) se encuentra en el Titular de la entidad del Sector Público de que se trate, figura que, como hemos visto, puede ser coincidente con la del Responsable del Servicio.

35. La determinación de los niveles 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.
36. La prestación de un servicio siempre debe atender a los requisitos de seguridad de la información que maneja (a veces se dice “se heredan los requisitos”), a los que se suele añadir requisitos de disponibilidad, accesibilidad, interoperabilidad, etc.

5.3. RESPONSABILIDADES UNIFICADAS

37. Como hemos señalado, es posible que coincidan en la misma persona u órgano colegiado las responsabilidades de la información y del servicio.
38. No obstante, 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.



Responsabilidades unificadas y separadas

6. NIVEL DE SUPERVISIÓN: EL RESPONSABLE DE LA SEGURIDAD

39. El Responsable de la Seguridad¹⁴ (de la información) es la persona designada por la Dirección de la entidad, según el procedimiento descrito en su Política de Seguridad de la Información.

¹⁴ Chief Information Security Officer (CISO): The person in charge of information security within the enterprise ISACA, Cybersecurity Glossary, 2014

Chief Information Security Officer (CISO): The CISO (chief information security officer) is a senior-level executive responsible for aligning security initiatives with enterprise programs and business objectives, ensuring that information assets and technologies are adequately protected (<http://whatis.techtarget.com/>)

Senior Agency Information Security Officer (SAISO): Official responsible for carrying out the Chief Information Officer responsibilities under the Federal Information Security Management Act (FISMA) and serving as the Chief Information Officer's primary liaison to the agency's authorizing officials, information system owners, and information systems security officers. (Note: Organizations subordinate to federal agencies may use the term Senior Information Security Officer or Chief Information Security Officer to denote individuals filling positions with similar responsibilities to Senior Agency Information Security Officers.) [CNSSI_4009:2010]

Senior (Agency) Information Security Officer: Official responsible for carrying out the Chief Information Officer responsibilities under FISMA and serving as the Chief Information Officer's primary liaison to the agency's

40. El ENS señala que el Responsable de la Seguridad determina las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios.
41. Además de ello, como hemos visto con anterioridad, en caso de servicios externalizados, la responsabilidad última la tiene siempre la Entidad del Sector Público destinataria de los servicios, aun cuando la responsabilidad inmediata pueda corresponder (vía contrato, convenio, encomienda, etc.) a la organización prestataria del servicio (lo que sucede, por ejemplo, en la utilización de servicios en la nube).
42. Las dos funciones esenciales del Responsable de la Seguridad son:
- 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 Información de la organización.
 - Promover la formación y concienciación en materia de seguridad de la información dentro de su ámbito de responsabilidad.
43. Además de ello, cuando la figura del Responsable de la Seguridad del ENS coincide con la **Entidad Responsable de Seguridad de la Información** derivada de la Directiva NIS¹⁵, podrá desplegar las siguientes funciones:
- Elaborar y proponer para aprobación por la organización las políticas de seguridad, que incluirán las medidas técnicas y organizativas, adecuadas y proporcionadas, para gestionar los riesgos que se planteen para la seguridad de las redes y sistemas de información utilizados y para prevenir y reducir al mínimo los efectos de los ciberincidentes que afecten a la organización y los servicios.
 - Desarrollar las políticas de seguridad, normativas y procedimientos derivados de la organización, supervisar su efectividad y llevar a cabo auditorías periódicas de seguridad.
 - Elaborar el documento de Declaración de Aplicabilidad.
 - Actuar como capacitador de buenas prácticas en seguridad de las redes y sistemas de información, tanto en aspectos físicos como lógicos.
 - Constituirse como punto de contacto con la autoridad competente en materia de seguridad de las redes y sistemas de información y responsable ante aquella del cumplimiento de las obligaciones que se derivan del RD-I 12/2018 y de su Reglamento de Desarrollo.
 - Constituir el punto de contacto especializado para la coordinación con el CSIRT de referencia.

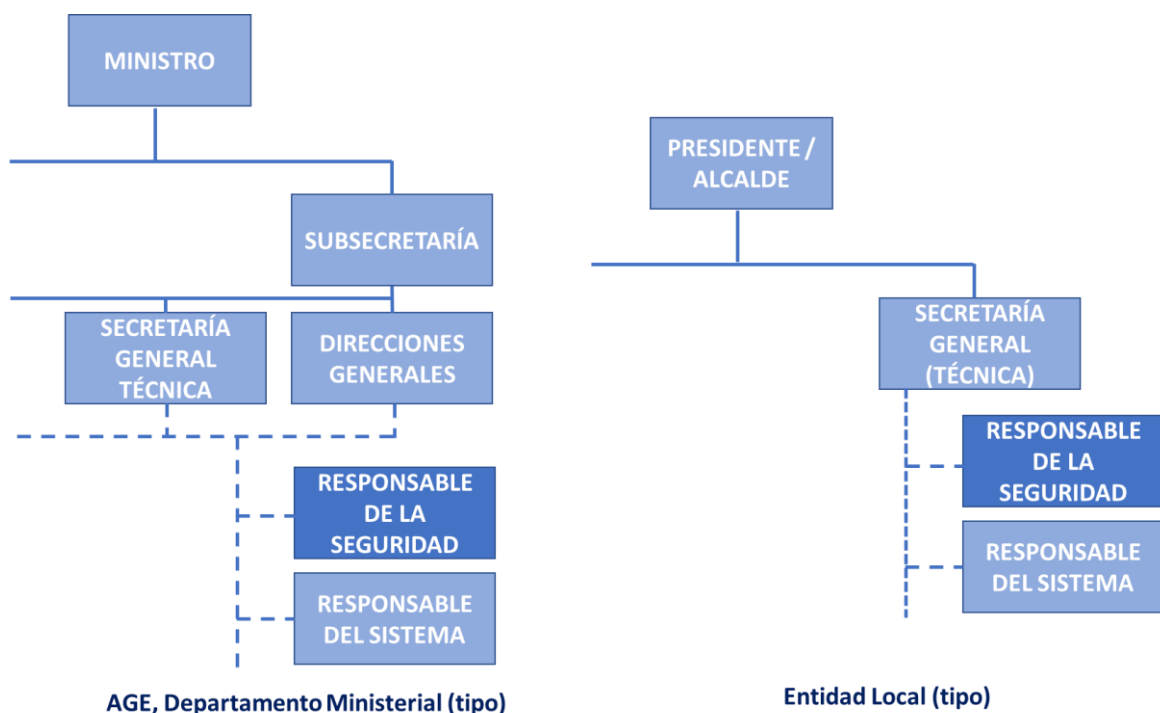
authorizing officials, information system owners, and information system security officers. (Note: Organizations subordinate to federal agencies may use the term Senior Information Security Officer or Chief Information Security Officer to denote individuals filling positions with similar responsibilities to Senior Agency Information Security Officers.) U.S. Code 44, Sec. 3544. Federal agency responsibilities, 2007

Chief Information Security Officer (CISO): The position of CISO is relatively new in most organizations. The CISO should be providing tactical information security advice and examining the ramifications of new technologies. In most corporations the CISO reports to the CIO or CTO. The CISO role does not usually include responsibility for physical security, risk management and business continuity, which are more often delegated to the CSO.

(<http://www.csoonline.com/glossary/>)

¹⁵ Transpuesta por Real Decreto-ley 12/2018, actualmente en fase de tramitación como Proyecto de Ley.

- Notificar a la autoridad competente, a través del CSIRT de referencia y sin dilación indebida, los incidentes que tengan efectos perturbadores en la prestación de los servicios.
 - Recibir, interpretar y aplicar las instrucciones y guías emanadas de la Autoridad Competente, tanto para la operativa habitual como para la subsanación de las deficiencias observadas.
 - Recopilar, preparar y suministrar información o documentación a la autoridad competente o el CSIRT de referencia, a su solicitud o por propia iniciativa.
44. Considerando que las leyes 39/2015 y 40/2015 consagran el uso de los medios electrónicos en el desenvolvimiento cotidiano de las entidades del Sector Público, parece lógico suponer que la figura del Responsable de la Seguridad debe estar situada en una posición que le permita tener un acceso directo a los niveles directivos de la organización. Por tanto, cuando se trate de organizaciones de la AGE, el Responsable de la Seguridad debería depender, en general, de la Secretaría General Técnica. En el caso de entidades locales (Diputaciones, Cabildos o Ayuntamientos), debería depender del Secretario General, tal como muestra la figura siguiente. En ambos casos, Secretaría General Técnica o Secretaría General liderarían los Comités de Seguridad de la Información.



45. En el caso de las Comunidades Autónomas dependerá del tipo de organización elegido para la función de seguridad de la información: vertical (seguridad de la información localizada en cada Consejería) o transversal (seguridad de la información como actividad horizontal). Si se quiere imprimir una transversalidad a la seguridad, una solución frecuentemente utilizada es situar la Responsabilidad de la Seguridad en el ámbito competencial de la Consejería encargada de la Administración Electrónica, ubicando Responsables de Seguridad Delegados en cada una de las Consejerías restantes.
46. En el caso de las Universidades, para asegurar el carácter transversal de la seguridad, el Responsable de la Seguridad corresponderá a un cargo o funcionario, de nivel ejecutivo, designado formalmente por el Rector o el Equipo de Dirección. El Responsable de la Seguridad no podrá ser un órgano de gobierno unipersonal de la Universidad y no deberá

- tener ninguna responsabilidad sobre la prestación de los servicios TIC, ni deberá estar bajo la dependencia jerárquica del Responsable del Sistema (y viceversa).
47. En aquellos sistemas de información que, por su complejidad, distribución, separación física de sus elementos o número de usuarios, se necesite de personal adicional para llevar a cabo las funciones de Responsable de la Seguridad, cada organización podrá designar **Responsables de Seguridad Delegados**. La designación corresponderá al Responsable de la Seguridad, que delegará funciones, no responsabilidad.
 48. Los Responsables de Seguridad Delegados se harán cargo, en su ámbito competencial, de todas aquellas funciones delegadas por el Responsable de la Seguridad. Es habitual que se encarguen de la seguridad de sistemas de información concretos (departamentales, por ejemplo) o de sistemas de información horizontales.
 49. Cada Responsable de la Seguridad Delegado mantendrá una dependencia funcional directa del Responsable de la Seguridad, a quien reportará.
 50. En entidades más grandes, no hay obstáculo para que la responsabilidad de la seguridad sea dirigida a través de un órgano colegiado, cuyo presidente, formalmente, será el Responsable de Seguridad en los términos expresados en el ENS, reflejados en la presente guía.
 51. El comité u órgano colegiado, podrá estar formado por todas aquellas personas con responsabilidad en materia de seguridad de la información (Responsable de Seguridad, Responsables de Seguridad Delegados, Responsables de seguridad por Aplicaciones o funciones verticales, sistemas, etc.), incluyendo, cuando sea el caso, a los responsables de seguridad de los sistemas de información externos que suministran servicios a la entidad pública de que se trate.

7. NIVEL OPERATIVO: EL RESPONSABLE DEL SISTEMA

7.1. EL RESPONSABLE DEL SISTEMA

52. El Responsable del Sistema¹⁶ será designado por la dirección de la entidad y su posición figurará en la Política de Seguridad de la Información de la entidad.
53. Tiene las siguientes funciones:
 - a. Desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida, incluyendo sus especificaciones, instalación y verificación de su correcto funcionamiento.
 - b. Definir la topología y la gestión del sistema de información, estableciendo los criterios de uso y los servicios disponibles en el mismo.
 - c. Cerciorarse de que las medidas de seguridad se integren adecuadamente en el marco general de seguridad.
54. El Responsable del Sistema puede proponer la suspensión del tratamiento de una cierta información o la prestación de un determinado servicio si aprecia deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos. La decisión final, que será tomada por la dirección de la entidad, debe ser acordada con los responsables de la información y los servicios afectados y el Responsable de la Seguridad.

¹⁶ Information System Owner (or Program Manager): Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system. [NIST-SP800-53:2013]

55. En determinados sistemas de información que, por su complejidad, distribución, separación física de sus elementos o número de usuarios se necesite de personal adicional para llevar a cabo las funciones de Responsable del Sistema, cada organización podrá designar cuantos **Responsables del Sistema Delegados** considere necesarios. La designación corresponde al Responsable del Sistema, que delega funciones, no responsabilidad.
56. Los Responsables del Sistema Delegados se harán cargo, en su ámbito competencial, de todas aquellas acciones delegadas por el Responsable del Sistema relacionadas con la operación, mantenimiento, instalación y verificación del correcto funcionamiento del sistema de información. Es habitual que estas figuras se encarguen de subsistemas de información de cierta envergadura o de sistemas de información que presten servicios horizontales.
57. Cada Responsable del Sistema Delegado mantendrá una dependencia funcional directa del Responsable del Sistema, a quien reportarán.

7.2. SEGURIDAD FÍSICA

58. Las medidas de protección de las instalaciones físicas pueden clasificarse en: **obstáculos físicos** (accesos físicos, torniquetes, puertas, candados, etc.); **técnicas de vigilancia** (sistemas de alarma, técnicas de vigilancia y monitorización); **sistemas de inteligencia** (herramientas de análisis y simulación de información basados en los datos extraídos de la monitorización); **vigilantes y personal de seguridad**.
59. Como quiera que el ENS contempla preceptos y medidas de seguridad específicos para la seguridad física, las entidades afectadas deberán desarrollar un marco conjunto capaz de dar respuesta a ambas exigencias: físicas y lógicas.
60. Así, el Responsable de la Seguridad Física adoptará 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.


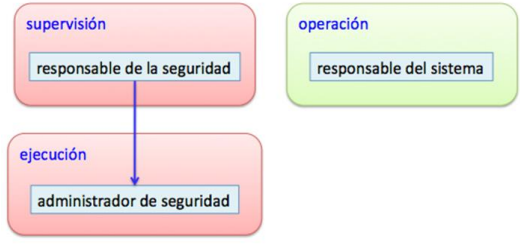
7.3. GESTIÓN DEL PERSONAL

61. Como quiera que el ENS también contempla preceptos y medidas de seguridad relativas al personal, los responsables de RR.HH. ajustarán sus acciones a lo establecido por el ENS en materia de seguridad ligada al personal, de forma análoga a lo establecido en los puntos anteriores.
62. El departamento de RR.HH. de la entidad adoptará las medidas de seguridad que le competan, dentro de las determinadas por el Responsable de la Seguridad de la Información, e informarán a éste de su grado de implantación, eficacia e incidentes.

8. EL ADMINISTRADOR DE SEGURIDAD (AS)

63. Atendiendo a la estructura organizativa de la entidad, el Administrador de Seguridad (AS) puede depender del Responsable del Sistema o del Responsable de la Seguridad.
64. Sus funciones más significativas serían las siguientes:
 - a. La implementación, gestión y mantenimiento de las medidas de seguridad aplicables al sistema de información.
 - b. La gestión, configuración y actualización, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad del sistema de información.

- c. La gestión de las autorizaciones y privilegios concedidos a los usuarios del sistema, incluyendo la monitorización de que la actividad desarrollada en el sistema se ajusta a lo autorizado.
 - d. La aplicación de los Procedimientos Operativos de Seguridad (POS).
 - e. Asegurar que los controles de seguridad establecidos son adecuadamente observados.
 - f. Asegurar que son aplicados los procedimientos aprobados para manejar el sistema de información.
 - g. Supervisar las instalaciones de hardware y software, sus modificaciones y mejoras para asegurar que la seguridad no está comprometida y que en todo momento se ajustan a las autorizaciones pertinentes.
 - h. Monitorizar el estado de seguridad del sistema proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica implementados en el sistema.
 - i. Informar al Responsable de la Seguridad o al Responsable del Sistema de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad.
 - j. Colaborar en la investigación y resolución de incidentes de seguridad, desde su detección hasta su resolución.
65. En emplazamientos donde se encuentren ubicados varios sistemas de información, la función de AS podría recaer en la misma persona, para todos ellos.
66. Como hemos señalado, el AS puede depender del Responsable del Sistema o del Responsable de la Seguridad (pero no de ambos). La tabla siguiente muestra las peculiaridades de ambas posiciones.

| AS en dependencia funcional del Responsable del Sistema | AS en dependencia funcional del Responsable de Seguridad |
|---|---|
|  |  |
| <p>Cuando el AS depende del Responsable del Sistema,</p> <ul style="list-style-type: none"> • La persona será designada por la Dirección a propuesta del Responsable del Sistema. • El AS reportará al Responsable del Sistema <p>Esta arquitectura es la clásica y prima las funciones operativas, en detrimento, en ocasiones, de las funciones de seguridad.</p> <p>Cuando se aplique, las actividades de auditoría deben incidir especialmente en garantizar un buen alineamiento entre los requisitos establecidos por el Responsable de Seguridad y las actuaciones del AS.</p> | <p>Cuando el AS depende del Responsable de la Seguridad,</p> <ul style="list-style-type: none"> • la persona será designada por la Dirección a propuesta del Responsable de la Seguridad. • El AS reportará al Responsable de la Seguridad. <p>Esta arquitectura es frecuente en sistemas donde la seguridad de la información es especialmente importante.</p> <p>Cuando se aplique, hay que asegurar que las funciones de explotación no se ven ralentizadas por las actividades del AS, estableciendo canales y foros de coordinación operativa.</p> |

| | |
|--|--|
| <p>Es posible segregar las funciones del AS en dos personas diferentes: una persona encargada del aseguramiento de la prestación del servicio (que dependería del Responsable del Sistema) y otra encargada de la protección de la información (que dependería del Responsable de la Seguridad).</p> | <p>Es posible segregar las funciones del AS en dos personas diferentes: una persona encargada del aseguramiento de la prestación del servicio (que dependería del Responsable del Sistema) y otra persona encargada de la protección de la información (que dependería del Responsable de la Seguridad).</p> <p>Cuando exista un AS que reporte al Responsable de la Seguridad, son funciones típicas las siguientes:</p> <ul style="list-style-type: none"> • Monitorización del estado de seguridad del sistema, analizando la información proporcionada por la herramienta de gestión de eventos de seguridad y mecanismos de auditoría técnica instalados en el sistema. • Supervisión de que todo el equipamiento se ajusta a lo autorizado. • Supervisión de las actividades de los administradores del sistema: actuaciones y aplicación de los procedimientos de seguridad establecidos. • Supervisión de que las actividades de los usuarios del sistema son conformes a lo autorizado para cada uno de ellos. • Cuando existe un sistema separado de gestión de privilegios, el AS puede encargarse de las actuaciones relativas a la implantación y mantenimiento de las autorizaciones concedidas a los usuarios del sistema. |
|--|--|

67. En determinados sistemas de información que, por su complejidad, distribución, separación física de sus elementos o número de usuarios, se necesite de personal adicional para llevar a cabo las funciones de AS, se podrán designar Administradores de Seguridad Delegados (AS-D).
68. Los AS-D serán responsables, en su ámbito competencial, de aquellas acciones que delegue el AS relacionadas con la implantación, gestión y mantenimiento de las medidas de seguridad aplicables al sistema de información.
69. El AS-D será designado a solicitud del AS, del que dependerá funcionalmente. Su identidad aparecerá reflejada en la documentación de seguridad del sistema de información.

9. COMITÉS

70. Como hemos señalado con anterioridad, algunas responsabilidades pueden instrumentalizarse por medio de Comités, que se constituirán como órganos colegiados, de conformidad con lo señalado en la Ley 40/2015. Estos Comités, que estarán formados por miembros de todas las partes implicadas, facilitan el desenvolvimiento de la organización y suelen ser habituales en entidades de tamaño mediano o grande.
71. Son habituales los siguientes:

- **Comité de Seguridad Corporativa**, que se responsabiliza de alinear todas las actividades de la organización en materia de seguridad, destacándose los aspectos de seguridad física y patrimonial (seguridad de las instalaciones), seguridad de la información, Compliance (seguridad y conformidad legal) y planes de contingencia.
- **Comité de Seguridad de la Información**, dependiente del anterior, que se responsabiliza de alinear las actividades de la organización en materia de seguridad de la información.

9.1. COMITÉ DE SEGURIDAD CORPORATIVA

72. La seguridad de la información es una más de las áreas de seguridad de una organización. En organizaciones de tamaño significativo suele existir un **Comité de Seguridad Corporativa** (con su propio Secretario, al que suele denominarse **Responsable de la Seguridad Corporativa (CSO)**). El Responsable de la Seguridad de la Información (CISO) será un miembro de este Comité, junto con otros **responsables de seguridad de otras áreas o departamentos**; por ejemplo:

- Responsables de Riesgos.
- Responsables de la Seguridad de Instalaciones (seguridad física).
- Responsables de Seguridad Industrial.
- Responsables de Seguridad Operacional.
- Responsables de Compliance legal.
- Responsables de Comunicación.
- Responsables de RR.HH.
- etc.

73. Son **funciones** típicas del Comité de Seguridad Corporativa las siguientes:

- Elaborar la Política de Seguridad Corporativa, que deberá ser aprobada por la Dirección de la entidad.
- Coordinar todas las funciones de seguridad de la organización.
- Velar por el cumplimiento de la normativa legal y sectorial de aplicación.
- Velar por el alineamiento de las actividades de seguridad a los objetivos de la organización.
- Coordinar los Planes de Continuidad de las diferentes áreas, para asegurar una actuación sin fisuras en caso de que deban ser activados.
- Coordinar y aprobar, en su caso, las propuestas de proyectos recibidas de los diferentes ámbitos de seguridad, encargándose gestionar un control y presentación regular del progreso de los proyectos y anuncio de las posibles desviaciones.
- Recibir las inquietudes en materia de seguridad de la Dirección de la entidad y transmitirlas a los responsables departamentales pertinentes, recabando de ellos las correspondientes respuestas y soluciones que, una vez coordinadas, habrán de ser comunicadas a la Dirección.
- Recabar de los responsables de seguridad departamentales informes regulares del estado de la seguridad de la organización y de los posibles incidentes. Estos informes, se consolidan y resumen para su comunicación a la Dirección de la entidad.
- Coordinar y dar respuesta a las inquietudes transmitidas a través de los responsables de seguridad departamentales.

- Definir, dentro de la Política de Seguridad Corporativa, la asignación de roles y los criterios para alcanzar las garantías pertinentes en lo relativo a segregación de funciones.
74. Como hemos señalado, el **Responsable de la Seguridad Corporativa (CSO)**¹⁷, actúa como Secretario del Comité de Seguridad Corporativa y entre sus cometidos se encuentran:
- Convoca al Comité de Seguridad Corporativa, recopilando la información pertinente.
 - Recaba las inquietudes de la Dirección de la entidad y de los responsables de seguridad departamentales, incorporándolas al Orden del Día del Comité de Seguridad Corporativa, para su examen y acciones pertinentes.
 - Es responsable, junto con los diferentes responsables de seguridad departamentales, de estar al tanto de cambios regulatorios o normativos (leyes, reglamentos o prácticas sectoriales) que afecten a la entidad, debiendo informarse de las consecuencias para las actividades de la organización, alertando al Comité de Seguridad Corporativa y proponiendo las medidas oportunas de adecuación al nuevo marco.
 - Es el responsable de la toma de decisiones cotidianas entre dos reuniones del Comité de Seguridad Corporativa. Estas decisiones darán respuesta a propuestas de los responsables de seguridad departamentales, velando por la unidad de acción y la coordinación de actuaciones, especialmente en caso de incidencias que tengan repercusión fuera de la organización y en caso de desastres.
75. Suele ser habitual que el Responsable de la Seguridad Corporativa se incorpore al **Comité de Crisis** en caso de desastre, coordinando todas las actuaciones relacionadas con cualquier aspecto de la seguridad de la organización.

9.2. COMITÉ DE SEGURIDAD DE LA INFORMACIÓN

76. La coordinación de la seguridad de la información en las entidades del Sector Público es especialmente importante por exigencia de racionalización del gasto y para evitar disfunciones que propicien la aparición de brechas de seguridad provocadas por puntos débiles en los sistemas de información que posibiliten incidentes accidentales o, incluso, ciberataques.
77. El **Comité de Seguridad de la Información** coordina la seguridad de la información en la entidad, y estará formado por el Responsable de la Seguridad (de la Información) y por representantes de otras áreas de la organización afectadas. La composición se determinará en la Política de Seguridad de la Información de la organización.
78. Son **funciones** típicas del Comité de Seguridad de la Información:
- Atender las inquietudes de la Dirección de la entidad y de los diferentes departamentos.
 - Informar regularmente del estado de la seguridad de la información a la Dirección.
 - Promover la mejora continua del sistema de gestión de la seguridad de la información.

¹⁷ Responsable de la Seguridad Corporativa: Persona encargada de velar por la armonización de la seguridad de la información en sus diferentes vertientes: protección física, protección de los servicios y respeto de la privacidad. Chief Security Officer (CSO): The person usually responsible for all security matters both physical and digital in an Enterprise. ISACA, Cybersecurity Glossary, 2014
Chief Security Officer (CSO): A CSO has the responsibility for global and enterprisewide information security; he/she is also responsible for the physical security, protection services and privacy of the corporation and its employees. In other words, the CSO is responsible for coordinating all corporate activities with security implications. (<http://www.csoonline.com/glossary/>)

- Elaborar la estrategia de evolución de la organización en lo que respecta a seguridad de la información.
 - Coordinar los esfuerzos de las diferentes áreas en materia de seguridad de la información, para asegurar que los esfuerzos son consistentes, que están alineados con la estrategia decidida en la materia, evitando duplicidades.
 - Elaborar (y revisar regularmente) la Política de Seguridad de la Información para su aprobación por la Dirección.
 - Aprobar la Normativa de Seguridad de la información.
 - Elaborar y aprobar los requisitos de formación y calificación de administradores, operadores y usuarios, desde el punto de vista de seguridad de la información.
 - Monitorizar los principales riesgos residuales asumidos por la organización y recomendar posibles actuaciones.
 - Monitorizar el desempeño de los procesos de gestión de incidentes de seguridad y recomendar posibles actuaciones respecto de ellos. En particular, velar por la coordinación de las diferentes áreas de seguridad en la gestión de tales incidentes.
 - Promover la realización de las auditorías periódicas que permitan verificar el cumplimiento de las obligaciones del organismo en materia de seguridad.
 - Aprobar planes de mejora de la seguridad de la información de la organización. En particular velará por la coordinación de distintos planes que puedan realizarse en diferentes áreas.
 - Priorizar las actuaciones en materia de seguridad cuando los recursos sean limitados.
 - Velar porque la seguridad de la información se tenga en cuenta en todos los proyectos TIC desde su especificación inicial hasta su puesta en operación. En particular, deberá velar por la creación y utilización de servicios horizontales que reduzcan duplicidades y apoyen un funcionamiento homogéneo de todos los sistemas TIC.
 - Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables y/o entre diferentes áreas de la organización, elevando aquellos casos en los que no tenga suficiente autoridad para decidir.
79. Puesto que el Comité de Seguridad de la Información no es un comité técnico, deberá recabar regularmente de personal técnico, propio o externo, la información pertinente para la toma de decisiones o asesoramiento. Este asesoramiento se determinará en cada caso, pudiendo materializarse de diferentes formas:
- Grupos de trabajo especializados, internos, externos o mixtos.
 - Asesoría externa.
 - Asistencia a cursos u otro tipo de eventos formativos o de intercambio de experiencias.
80. El Responsable de la Seguridad (del ENS) será el secretario del Comité de Seguridad de la Información, y como tal:
- Convoca las reuniones del Comité de Seguridad de la Información.
 - Prepara los temas a tratar en las reuniones del Comité, aportando información puntual para la toma de decisiones.
 - Elabora el acta de las reuniones.
 - Es responsable de la ejecución directa o delegada de las decisiones del Comité.

10. NOMBRAMIENTOS

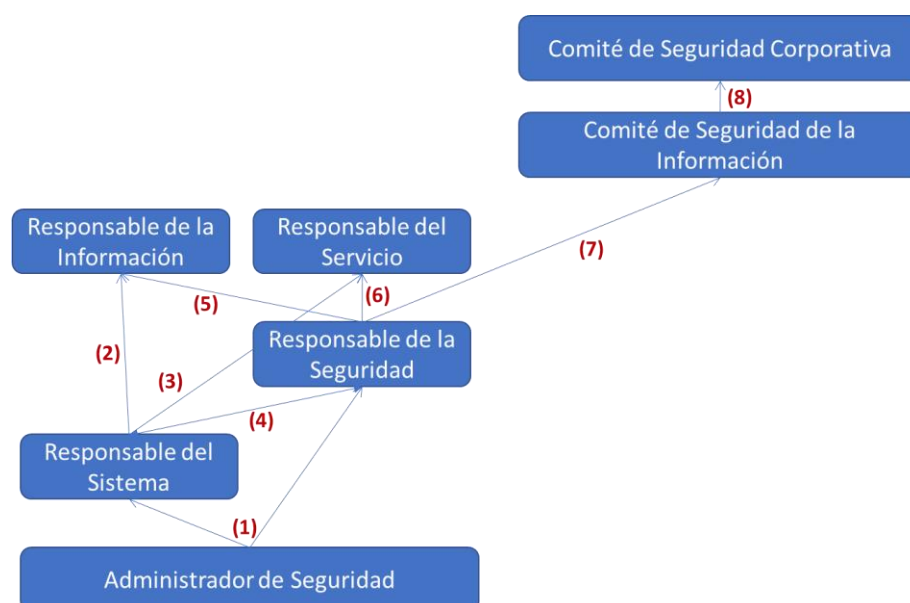
81. Es función de la Dirección de la entidad designar:
- Al Responsable de la Información, que puede ser un cargo unipersonal o un órgano colegiado (integrado, habitualmente, en Comité de Seguridad de la Información).
 - Al Responsable del Servicio, que, pudiendo ser el mismo que el Responsable de la Información, también puede ser un cargo unipersonal o un órgano colegiado (integrado, habitualmente, en Comité de Seguridad de la Información).
 - Al Responsable de la Seguridad, que debe reportar directamente a la Dirección o a los órganos de gobierno de la entidad y, cuando existan, a los Comités de Seguridad Corporativa y de Seguridad de la Información.
 - Al Responsable del Sistema, que, en materia de seguridad, reportará al Responsable de la Seguridad. Esta designación podrá ser:
 - 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 trate diferentes informaciones o preste diferentes servicios, oídos los responsables de las informaciones y los servicios afectados.
 - Al Administrador de Seguridad, a propuesta del Responsable del Sistema (ver opciones de dependencia en la sección dedicada al AS)¹⁸.
82. El procedimiento de nombramiento de los responsables mencionados en el párrafo anterior debe constar en la Política de Seguridad de la Información de la entidad, y debe revestir el carácter de formal.

11. REPORTES Y FLUJO DE INFORMACIÓN

83. Los números representan las flechas señaladas en el gráfico siguiente.
84. (1) El Administrador de Seguridad, reportará al Responsable del Sistema o al Responsable de la Seguridad, según su dependencia funcional, de los incidentes relativos a la seguridad del sistema y de las acciones de configuración, actualización o corrección.
85. (2) El Responsable del Sistema reportará al Responsable de la Información de las incidencias funcionales relativas a la información que le compete.
86. (3) El Responsable del Sistema reportará al Responsable del Servicio de las incidencias funcionales relativas al servicio que le compete.
87. (4) El Responsable del Sistema reportará al Responsable de la Seguridad de las actuaciones en materia de seguridad, en particular en lo relativo a decisiones de arquitectura del sistema y le entregará un resumen consolidado de los incidentes de seguridad.

¹⁸ Es 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.

88. (4) Cuando el AS 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.
89. (4) Cuando el AS dependa del Responsable de la Seguridad, éste proporcionará al Responsable del Sistema un resumen consolidado de los incidentes de seguridad.
90. (5) El Responsable de la Seguridad reportará al Responsable de la Información las decisiones e incidentes en materia de seguridad que afecten a la información que le compete, en particular de la estimación de riesgo residual y de las desviaciones significativas de riesgo respecto de los márgenes aprobados.
91. (6) El Responsable de la Seguridad reportará al Responsable del Servicio las decisiones e incidentes en materia de seguridad que afecten al servicio que le compete, en particular de la estimación de riesgo residual y de las desviaciones significativas de riesgo respecto de los márgenes aprobados.
92. (7) Cuando exista un Comité de Seguridad de la Información, el Responsable de la Seguridad reportará a dicho Comité, en su calidad de Secretario, entregando un resumen consolidado de actuaciones en materia de seguridad y de los incidentes relativos a la seguridad de la información, e informándole del estado de la seguridad del sistema, en particular del riesgo residual al que el sistema está expuesto.
93. (8) Cuando exista un Comité de Seguridad Corporativa, el Responsable de la Seguridad informará a dicho Comité como miembro, según lo acordado en el Comité de Seguridad de la Información.
94. Cuando no exista un Comité de Seguridad Corporativa, el Responsable de la Seguridad informará a la Dirección de la entidad, según lo acordado en el Comité de Seguridad de la Información.
95. Cuando no exista un Comité de Seguridad de la Información, el Responsable de la Seguridad reportará directamente a la Dirección de la entidad, entregándole un resumen consolidado de actuaciones en materia de seguridad y de los incidentes relativos a la seguridad de la información, e informándole del estado de la seguridad del sistema, en particular del riesgo residual al que el sistema está expuesto.



12. GESTIÓN DE LOS RIESGOS

96. La gestión de los riesgos es una tarea que debe realizarse de manera continua sobre los sistemas de información y orientar todas las restantes actividades de acuerdo a los principios “Gestión de riesgos” y “Reevaluación periódica”¹⁹.
97. La forma de realizar el análisis de riesgos se detalla en el Anexo II del ENS, medida [op.pl.1] “Análisis de riesgos”, estableciendo una proporcionalidad entre el nivel de detalle del análisis y la categoría del sistema de información²⁰.
98. El Responsable de la Información es el propietario de los riesgos sobre la información.
99. El Responsable del Servicio es el propietario de los riesgos sobre los servicios.
100. 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 propietario²¹.
101. **Indicadores de riesgo**²². En sistemas de información de categoría alta se recomienda que se establezcan indicadores del estado de los riesgos críticos (*KRI – Key Risk Indicators*). Tales indicadores:

¹⁹ Ver artículo 6 del ENS (“Gestión de la seguridad basada en los riesgos”) y artículo 9 (“Reevaluación periódica”)

²⁰ Véase el Anexo A: Tareas, donde se muestran escenarios posibles de asignación de tareas relativas a la gestión de riesgos.

²¹ Naturalmente, en última instancia, es el Titular de la entidad pública de que se trate el responsable de aceptar los riesgos residuales o solicitar medidas adicionales de mitigación de tal riesgo residual.

²² Indicador de Riesgos Clave: Un indicador de riesgos clave (KRI) es una métrica para determinar qué tan posible es que la probabilidad de un evento, combinada con sus consecuencias, supere el apetito de riesgo de la organización (es decir, el nivel de riesgo que la compañía está preparada para aceptar), y tenga un impacto profundamente negativo en la capacidad de tener éxito de una organización. Si una organización se especializa en ventas al por menor, por ejemplo, un indicador de riesgo clave podría ser el número de quejas de los clientes, porque el aumento de este KRI podría ser una indicación temprana de que hay que resolver un problema operativo.

El desafío para una organización no es solo identificar cuáles indicadores de riesgo deben ser identificados como claves (los más importantes), sino también comunicar esa información de tal manera que todo el mundo en la organización entienda claramente su significado. Identificar indicadores de riesgos clave requiere la comprensión de las metas de la organización.

Cada KRI debería ser capaz de ser medido con precisión y reflejar de manera precisa el impacto negativo que tendría sobre los indicadores de desempeño clave de la organización (KPI). Los indicadores de rendimiento clave, que a menudo se confunden con los indicadores de riesgos clave, son las métricas que ayudan a una organización a evaluar el progreso hacia los objetivos declarados. (<http://searchdatacenter.techtarget.com/es/>) CCN-STIC-401 Glosario y Abreviaturas.

Key Risk Indicator (KRI): A subset of risk indicators that are highly relevant and possess a high probability of predicting or indicating important risk. ISACA, Cybersecurity Glossary, 2014

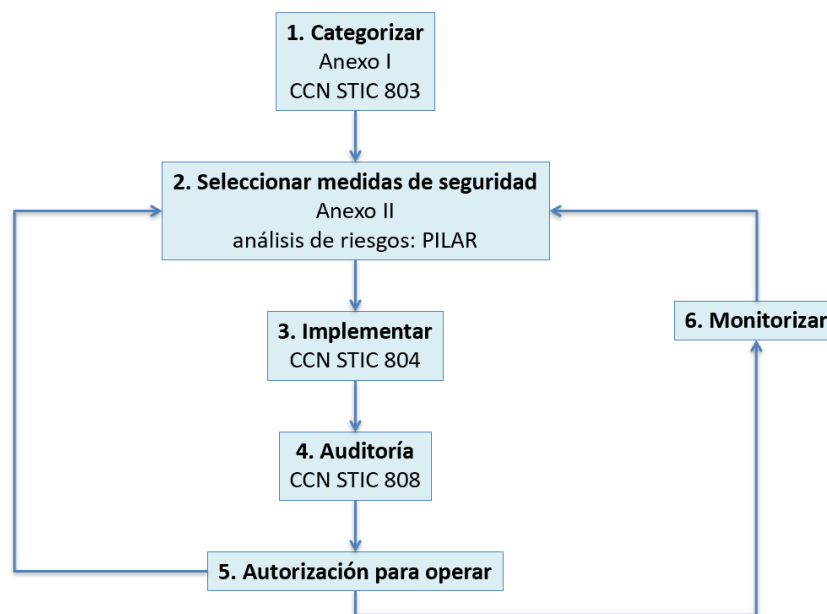
Key Risk Indicator (KRI): An enterprise may develop an extensive set of metrics to serve as risk indicators; however, it is not possible or feasible to maintain that full set of metrics as key risk indicators (KRIs). KRIs are differentiated as being highly relevant and possessing a high probability of predicting or indicating important risk. The Risk IT Practitioner Guide. November 2009.

Key Risk Indicator (KRI): A key risk indicator (KRI) is a metric for measuring the likelihood that the combined probability of an event and its consequence will exceed the organization's risk appetite and have a profoundly negative impact on an organization's ability to be successful.

If an organization specializes in retail sales, for example, a key risk indicator might be the number of customer complaints because increase in this KRI could be an early indication that an operational problem needs to be addressed. The challenge for an organization is not only to identify which risk indicators should be identified as being key (most important) but also to communicate that information in such a way that everyone in the organization clearly understands its significance.

Identifying key risk indicators requires an understanding of the organization's goals. Each KRI should be able to be measured and accurately reflect the negative impact it would have on the organization's key performance indicators

- Son propuestos por el Responsable de la Seguridad.
 - Su definición es acordada por el Responsable de la Seguridad y el propietario del riesgo. La definición indicará, exactamente:
 - En qué medidas se basan.
 - Cuál es el algoritmo de cálculo.
 - La periodicidad de evaluación y
 - Los umbrales de aviso y alarma (atención urgente).
 - Se presentan al responsable correspondiente
 - Rutinariamente, con la periodicidad establecida.
 - Puntualmente, por demanda del propietario del riesgo medido, y
 - Extraordinariamente, cuando se supera un determinado umbral de riesgo.
 - Estos indicadores estarán a disposición de los auditores.
102. 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.



Proceso de Gestión de Riesgos

(KPIs). Key performance indicators, which are often confused with key risk indicators, are metrics that help an organization assess progress towards declared goals. (<http://searchcio.techtarget.com/>)

Key Risk Indicator (KRI): A Key Risk Indicator, also known as a KRI, is a measure used in management to indicate how risky an activity is. It differs from a Key Performance Indicator (KPI) in that the latter is meant as a measure of how well something is being done while the former is an indicator of the possibility of future adverse impact. KRI give us an early warning to identify potential event that may harm continuity of the activity/project. (http://en.wikipedia.org/wiki/Key_Risk_Indicator)

Proceso de Gestión de Riesgos:**103. Paso 1 – Categorizar el sistema de información:**

- El Responsable de la Información manejada establece los niveles requeridos²³.
- El Responsable de los Servicios prestados establece los niveles requeridos²⁴.
- Se deduce, automáticamente, la categoría del sistema de información²⁵.

104. Paso 2 – Seleccionar las medidas de seguridad:

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

105. Paso 3 – Implementar las medidas de seguridad:

- El Administrador de Seguridad (AS) se encarga de aplicar las medidas acordadas²⁶.

106. Paso 4 – Evaluar la seguridad del sistema de información:

- Corresponde al sistema de gestión que se emplee, pudiendo recurrir a auditorías externas cuando sea pertinente²⁷.

107. 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.

108. Paso 6 – Monitorizar:

- El Administrador de Seguridad (AS) recopila información sobre el desempeño del sistema de información en materia de seguridad.
- El Responsable de la 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 las desviaciones son elevadas, el Responsable del Sistema puede acordar la suspensión temporal del servicio hasta que se puedan garantizar niveles aceptables de riesgo²⁸.

²³ Ver Anexo I del ENS y guía CCN-STIC 803. Esta acción es igualmente aplicable al Responsable del Tratamiento de datos personales.

²⁴ Ver Anexo I del ENS y guía CCN-STIC 803.

²⁵ Ver Anexo I del ENS.

²⁶ Ver guía CCN STIC 804. No obstante, algunas de tales medidas podrían salir de su ámbito y ser implementadas por otros.

²⁷ Ver guía CCN STIC 802.

²⁸ Recordamos que, en última instancia, es la Dirección de la entidad pública la que, administrativamente, está competencialmente autorizada para suspender la prestación de los servicios.

13. CONCURRENCIA CON EL RGPD

109. Esta sección trata de los puntos de contacto del ENS con el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos - RGPD)²⁹.
110. Como hemos señalado al comienzo de esta Guía, el RGPD identifica varios roles:
- **Responsable del Tratamiento** (Art. 4). «responsable del tratamiento» o «responsable»: la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros;
 - **Encargado del Tratamiento** (Art.4). «encargado del tratamiento» o «encargado»: la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento;
 - **Delegado de Protección de Datos (DPD)** (Art. 37).
111. Aunque la figura del DPD se menciona frecuentemente en la norma, son de especial relevancia los artículos 37 y 39 de la Sección 4.
112. Así, el artículo 37 indica que el DPD es un rol externalizable³⁰.
113. Por su parte, el artículo 39 delimita sus funciones³¹.

²⁹ Para más detalles, véase la Guía CCN-STIC 881 Impacto del RGPD en el ENS.

³⁰ **Artículo 37. Designación del Delegado de Protección de Datos**

...
5. El Delegado de Protección de Datos será designado atendiendo a sus cualidades profesionales y, en particular, a sus conocimientos especializados del Derecho y la práctica en materia de protección de datos y a su capacidad para desempeñar las funciones indicadas en el artículo 39.

6. El Delegado de Protección de Datos podrá formar parte de la plantilla del responsable o del encargado del tratamiento o desempeñar sus funciones en el marco de un contrato de servicios.

³¹ **Artículo 39 - Funciones del Delegado de Protección de Datos**

1. El Delegado de Protección de Datos tendrá como mínimo las siguientes funciones:

a) informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben en virtud del presente Reglamento y de otras disposiciones de protección de datos de la Unión o de los Estados miembros;

b) supervisar el cumplimiento de lo dispuesto en el presente Reglamento, de otras disposiciones de protección de datos de la Unión o de los Estados miembros y de las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes;

c) ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación de conformidad con el artículo 35;

d) cooperar con la autoridad de control;

e) actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa a que se refiere el artículo 36, y realizar consultas, en su caso, sobre cualquier otro asunto.

2. El Delegado de Protección de Datos desempeñará sus funciones prestando la debida atención a los riesgos asociados a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y fines del tratamiento.

114. La faceta de supervisión del DPD exige que sea una entidad diferente de la supervisada, de forma que si las funciones de tratamiento recaen en el Responsable del Sistema, este no puede asumir las funciones de DPD.
115. Por otra parte, en determinadas circunstancias, no es incompatible que el DPD coincida con el Responsable de la Seguridad del ENS, como se ha mencionado en el epígrafe 3 de la presente Guía.
116. Finalmente, recordar que la figura del DPD puede constituirse a través de un órgano colegiado (adoptando la forma de un Comité Delegado de Protección de Datos), pudiendo contar entre sus miembros con expertos externos -personas físicas o jurídicas-, especializados en seguridad de la información y protección de datos, siempre que quede garantizada la inexistencia de conflicto de intereses entre sus miembros.

ANEXO A. RESPUESTA A INCIDENTES Y MATRIZ RACI

RESPUESTA A INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

- AS: Llevar a cabo el registro, contabilidad y gestión de los incidentes de seguridad en los sistemas de información bajo su responsabilidad.
- AS: Aislar el incidente para evitar la propagación a elementos ajenos a la situación de riesgo.
- AS: Tomar decisiones a corto plazo si la información se ha visto comprometida y pudiera tener consecuencias graves (estas actuaciones deberían estar procedimentadas para reducir el margen de discrecionalidad del AS al mínimo).
- AS: Asegurar la integridad de los elementos críticos del sistema de información si se ha visto afectada la disponibilidad de los mismos (estas actuaciones deberían estar procedimentadas para reducir el margen de discrecionalidad del AS al mínimo).
- AS: Mantener y recuperar la información almacenada por el sistema de información y sus servicios asociados.
- AS: Investigar el incidente: determinar el modo, los medios, los motivos y el origen del incidente.
- RSEG: Analizar y proponer salvaguardas que prevengan incidentes similares en el futuro.
- RSIS: Planificar la implantación de las salvaguardas en el sistema.
- Comité de Seguridad de la Información: Proponer para su aprobación por la Dirección, el Plan de Mejora de la Seguridad, con su dotación presupuestaria correspondiente.
- RSIS: Ejecutar el plan de mejora de la seguridad aprobado.
- Responsable del tratamiento: En aquellos incidentes de seguridad que afecten también a datos de carácter personal, se deberán notificar a la AEPD y, en su caso, a los ciudadanos, sin perjuicio de que el DPD esté informado y actúe como interlocutor del Responsable del tratamiento ante la AEPD y las autoridades autonómicas de protección de datos.

MATRIZ RACI

La matriz RACI que se expone a continuación es orientativa y cada entidad deberá adecuarla a su organización particular.

La matriz de la asignación de responsabilidades (RACI, por las iniciales inglesas de los tipos de responsabilidad) se utiliza generalmente en la gestión de proyectos para relacionar actividades con recursos (individuos o equipos de trabajo). De esta manera, se logra asegurar que cada una de las tareas esté asignada a un individuo o a un equipo.

| | 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 | |

Debemos entender la “suspensión cautelar del servicio” como una respuesta ágil ante un problema de seguridad detectado, y de corta duración. Si fuera de larga duración, la aprobación de la suspensión debería recaer en la Dirección de la organización, siendo consultados los RINFO, RSERV y RSEG, y siendo responsable de su ejecución el RSIS.

Algunas tareas carecen de R porque no entra dentro del alcance de esta guía establecer quién se encarga de su realización. No obstante, en cada entidad se deberá determinar quién se encarga de cada tarea o cómo se subdivide hasta poder concretar.

ANEXO B. ESTRUCTURAS POSIBLES DE IMPLANTACIÓN

| Estructura Mínima | Estructura Intermedia | Estructura Deseable |
|--|--|---|
| En organismos de tamaño o recursos reducidos, las responsabilidades identificadas en esta guía pueden implementarse en dos roles: | En organismos de dimensión intermedia, las responsabilidades identificadas en esta guía pueden implementarse en tres roles: | Contando con uno o varios Comités de Seguridad de la Información y de Protección de Datos que contemplen las siguientes responsabilidades: |
| Gobierno y Supervisión: una figura integrando las siguientes funciones: <ul style="list-style-type: none"> Responsable del Tratamiento (si hay datos de carácter personal). Responsable de la Información. Responsable del Servicio. Responsable de la Seguridad. | Gobierno: una figura integrando las siguientes funciones: <ul style="list-style-type: none"> Responsable del Tratamiento (si hay datos de carácter personal). Responsable de la Información. Responsable del Servicio. | <ul style="list-style-type: none"> Responsabilidades derivadas del tratamiento de datos de carácter personal. Responsables de Información, para todas las informaciones manejadas por los servicios prestados dentro del marco de las leyes que puedan resultar de aplicación³². Responsables de Servicios, para todos los servicios prestados dentro del marco de las leyes que puedan resultar de aplicación. |
| <ul style="list-style-type: none"> Delegado de Protección de Datos. | <ul style="list-style-type: none"> Delegado de Protección de Datos. | |
| | Supervisión: una figura, reportando a Dirección, y desarrollando la función de: <ul style="list-style-type: none"> Responsable de la Seguridad. | Supervisión: una figura, reportando a Dirección, y desarrollando la función de: <ul style="list-style-type: none"> Responsable de la Seguridad. |
| Operación: una figura, reportando a Dirección, e integrando las siguientes funciones: <ul style="list-style-type: none"> Responsable del Sistema. Administrador de Seguridad. | Operación: una figura, reportando a Dirección, e integrando las siguientes funciones: <ul style="list-style-type: none"> Responsable del Sistema. Administrador de Seguridad. | Operación: una figura, reportando a Dirección, e integrando las siguientes funciones: <ul style="list-style-type: none"> Responsable del Sistema. Administrador de Seguridad. |

³² RGPD, Ley Orgánica 3/2018 LOPDGDD, Leyes 39/2015 y 40/2015; ENS, RD-I 12/2018, etc.