







seguridad se atajen a tiempo. Las medidas de recuperación permitirán la restauración de la información y los servicios.

2. Las directrices fundamentales de seguridad se concretan en un conjunto de principios particulares y responsabilidades específicas, que se configuran como objetivos instrumentales que garantizan el cumplimiento de los principios básicos de la PSI y que inspiran las actuaciones de la Comisión Nacional de los Mercados y la Competencia en dicha materia. Se establecen los siguientes:

- a) Protección de datos de carácter personal: Se adoptarán las medidas técnicas y organizativas que corresponda implantar para atender los riesgos generados por el tratamiento de acuerdo a lo exigido por 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).
- b) Gestión de activos de información: Los activos de información de la Comisión Nacional de los Mercados y la Competencia se encontrarán inventariados y categorizados y estarán asociados a un responsable.
- c) Seguridad ligada a las personas: Se implantarán los mecanismos necesarios para que cualquier persona que acceda, o pueda acceder a los activos de información, conozca sus responsabilidades y de este modo se reduzca el riesgo derivado de un uso indebido de dichos activos.
- d) Seguridad física: Los activos de información serán emplazados en áreas seguras, protegidas por controles de acceso físicos adecuados a su nivel de criticidad. Los sistemas y los activos de información que contienen dichas áreas estarán suficientemente protegidos frente a amenazas físicas o ambientales.
- e) Seguridad en la gestión de comunicaciones y operaciones: Se establecerán los procedimientos necesarios para lograr una adecuada gestión de la seguridad, operación y actualización de las Tecnologías de la Información y Comunicaciones. La información que se transmita a través de redes de comunicaciones deberá ser adecuadamente protegida, teniendo en cuenta su nivel de sensibilidad y de criticidad, mediante mecanismos que garanticen su seguridad.
- f) Control de acceso: Se limitará el acceso a los activos de información por parte de usuarios, procesos y otros sistemas de información mediante la implantación de los mecanismos de identificación, autenticación y autorización acordes a la criticidad de cada activo. Además, quedará registrada la utilización del sistema con objeto de asegurar la trazabilidad del acceso y auditar su uso adecuado, conforme a la actividad de la organización.

- g) Adquisición, desarrollo y mantenimiento de los sistemas de información: Se contemplarán los aspectos de seguridad de la información en todas las fases del ciclo de vida de los sistemas de información, garantizando su seguridad por defecto.
- h) Gestión de los incidentes de seguridad: Se implantarán los mecanismos apropiados para la correcta identificación, registro y resolución de los incidentes de seguridad.
- i) Gestión de la continuidad: Se implantarán los mecanismos apropiados para asegurar la disponibilidad de los sistemas de información y mantener la continuidad de sus procesos de negocio, de acuerdo a las necesidades de nivel de servicio de sus usuarios.
- j) Cumplimiento: Se adoptarán las medidas técnicas, organizativas y procedimentales necesarias para el cumplimiento de la normativa legal vigente en materia de seguridad de la información.

#### Artículo 5. Estructura organizativa.

1. La estructura organizativa para la gestión de la seguridad de la información en el ámbito descrito por la PSI de la Comisión Nacional de los Mercados y la Competencia está compuesta por los siguientes agentes:

- a) La Comisión de Seguridad de la Información.
- b) El Responsable de Seguridad.
- c) Los Responsables de la Información.
- d) Los Responsables del Servicio.
- e) El Responsable del Sistema.

2. La estructura organizativa será competente para mantener, actualizar y hacer cumplir, dentro del ámbito definido por la presente Resolución, la PSI de la Comisión Nacional de los Mercados y la Competencia.

#### Artículo 6. La Comisión de Seguridad de la Información.

1. Adscrito a la Secretaría General, se crea la Comisión de Seguridad de la Información (en adelante CSI), como órgano colegiado de los previstos en el artículo 20.3 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, que gestionará y coordinará todas las actividades relacionadas con la seguridad de los sistemas de información.

2. La CSI estará compuesto por los siguientes miembros:

- k) Presidente: El titular de la Secretaría General. Tendrá voto de calidad en la toma de decisiones del Comité.
- l) Vicepresidente: El titular de la Subdirección de Sistemas y Tecnologías de la Información y las Comunicaciones.
- m) Vocales: Un representante de cada una de las siguientes direcciones o departamentos. Serán nombrados por el Presidente de la Comisión Nacional de los Mercados y la Competencia a propuesta del titular de la dirección o departamento, de entre el personal funcionario o laboral, con rango mínimo de Subdirector o equivalente:
  - i. Gabinete del Presidente
  - ii. Secretaría del Consejo
  - iii. Dirección de Competencia
  - iv. Dirección de Energía
  - v. Dirección de Telecomunicaciones y del Sector Audiovisual
  - vi. Dirección de Transportes y del Sector postal
  - vii. Departamento de Promoción de la Competencia
  - viii. Departamento de Control Interno
  - ix. El Delegado de Protección de Datos, si no estuviera ya representado en la CSI.

c) Secretario: un empleado público de cuerpo A1 o equivalente de la Subdirección de Sistemas y Tecnologías de la Información y las Comunicaciones, que tendrá voz y voto y que ejecutará las decisiones del Comité, convocará sus reuniones y preparará los temas a tratar. Será nombrado por el Presidente a propuesta de la Secretaria General.

Para cada miembro del Comité se designará un suplente, con rango mínimo de Subdirector Adjunto o equivalente, que sustituirá al miembro principal en caso de que acontezca una causa justificada. Estos suplentes serán nombrados igualmente por el Presidente de la Comisión Nacional de los Mercados y la Competencia.

El Presidente del Comité podrá autorizar la asistencia a las reuniones de expertos en las materias que se vayan a tratar, que tendrán el carácter de asesores, con voz, pero sin voto.

3. La CSI ejercerá las siguientes funciones:

- a) Aprobar las propuestas de modificación y actualización permanente de la PSI de la Comisión Nacional de los Mercados y la Competencia e impulsar su cumplimiento. Dichas propuestas deberán ser elevadas al Presidente de la Comisión Nacional de los Mercados y la Competencia para su firma y posterior publicación.
- b) Aprobar las normas de desarrollo de la PSI de segundo nivel, según lo previsto en el artículo 15 de esta Resolución e impulsar su cumplimiento.

- c) Aprobar el Plan de Auditoría y el plan de Formación en materia de seguridad propuestos por el Responsable de Seguridad. En lo que se refiere a la aprobación del Plan de Auditoría en materia de seguridad, la CSI actuará en coordinación con el Departamento de Control Interno.
- d) Resolver los posibles conflictos que puedan derivarse del establecimiento de la citada estructura organizativa.

4. La CSI se reunirá con carácter ordinario al menos una vez al año y con carácter extraordinario cuando lo decida su Presidente. En cuanto a su funcionamiento, se regirá, en todo lo no previsto en la presente Resolución, por lo dispuesto en el Capítulo II, Sección 3ª, del Título Preliminar de la Ley 40/2015, de 1 de octubre, ya citada, que regula el funcionamiento de los órganos colegiados de la Administración.

5. La CSI podrá recabar de personal técnico, propio o externo, la información pertinente para la toma de sus decisiones.

#### Artículo 7. El Responsable de Seguridad.

1. El Responsable de Seguridad es la persona que determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios.
2. El Presidente designará al Responsable de Seguridad.
3. Serán funciones del Responsable de Seguridad las siguientes:
  - a) Promover la seguridad de la información manejada y de los servicios electrónicos prestados por los sistemas de información.
  - b) Elaborar estudios, análisis previos y propuestas de modificación y actualización de la PSI.
  - c) Analizar el cumplimiento de la PSI y de su desarrollo normativo.
  - d) Elaborar las directrices de seguridad de segundo nivel definidas en el artículo 15 de la presente Resolución y aprobar los procedimientos e instrucciones que constituyen el tercer nivel.
  - e) Velar e impulsar el cumplimiento del cuerpo normativo definido en el artículo 15 de la presente Resolución.
  - f) Coordinar la comunicación con los Centros de servicios de respuesta de incidentes de seguridad que corresponda.

- g) Apoyar y supervisar la investigación de los incidentes de seguridad desde su notificación hasta su resolución y participar en la toma de decisiones en momentos de alerta.
- h) Encargarse de que la documentación de seguridad se mantenga organizada y actualizada, y de gestionar los mecanismos de acceso a la misma.
- i) Promover la mejora continua en la gestión de la seguridad de la información.
- j) Seguimiento de las medidas resultado del análisis y gestión de riesgos de los activos.
- k) Impulsar la formación y concienciación en materia de seguridad de la información.
- l) Proponer la categoría del sistema según el procedimiento descrito en el anexo I del Real Decreto 3/2010, de 8 de enero y las medidas de seguridad que deben aplicarse de acuerdo con lo previsto en el anexo II del mismo real decreto.
- m) Promover auditorías periódicas para verificar el cumplimiento de las obligaciones en materia de seguridad de la información. Para esta función se apoyará en las actuaciones que el Departamento de Control Interno pueda llevar a cabo en esta materia.
- n) Realizar el seguimiento y control del estado de seguridad del sistema de información.
- o) Verificar que las medidas de seguridad son adecuadas para la protección de la información y los servicios.
- p) Elaborar informes periódicos de seguridad para el Comité que incluyan los incidentes más relevantes de cada período.
- q) Asumir las funciones explícitamente atribuidas a la figura del Responsable de Seguridad en el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad.

#### Artículo 8. Equipo de Seguridad.

1. El Equipo de Seguridad es un grupo de apoyo al Responsable de Seguridad para el cumplimiento de sus funciones, que aglutinará los esfuerzos de prevención de incidentes de seguridad, detección de anomalías, mecanismos de respuesta eficaz ante los mismos y actividades de recuperación mediante el desarrollo de planes de continuidad de los sistemas de información para garantizar la disponibilidad de los servicios críticos.



2. A estos efectos, el Equipo de Seguridad realizará las auditorías periódicas de seguridad, el seguimiento y control del estado de seguridad de los sistemas y servicios, la respuesta eficaz a los incidentes de seguridad desde su notificación hasta su resolución y el desarrollo de los planes de continuidad de los sistemas de información.

3. Los componentes del Equipo de Seguridad se determinarán por el Responsable de Seguridad, de entre los efectivos que presten servicio en la Subdirección de Sistemas y Tecnologías de la Información y las Comunicaciones a propuesta del titular de dicha Subdirección.

#### Artículo 9. Los Responsables de la Información.

1. Los Responsables de la Información tienen la potestad, dentro de su ámbito de actuación y de sus competencias, de establecer los requisitos, en materia de seguridad, de la información que manejan. Si esta información incluye datos de carácter personal, además deberán tenerse en cuenta las medidas de seguridad que corresponda implantar atendidos los riesgos generados por el tratamiento de acuerdo a lo exigido por el citado Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016.

2. Las funciones de Responsable de la Información recaerán en el titular de la unidad administrativa que gestione cada procedimiento administrativo, pudiendo una misma persona acumular las responsabilidades de la información de todos los procedimientos que gestione.

#### Artículo 10. Los Responsables del Servicio.

1. Los Responsables del Servicio tienen la potestad, dentro de su ámbito de actuación y de sus competencias, de establecer los requisitos, en materia de seguridad, de los servicios. Si estos servicios incluyen datos de carácter personal, además deberán tenerse en cuenta las medidas de seguridad que corresponda implantar atendidos los riesgos generados por el tratamiento de acuerdo a lo exigido por el citado Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016.

2. Las funciones de Responsable del Servicio recaerán en el titular de la unidad administrativa que gestione cada procedimiento administrativo, pudiendo una misma persona acumular las responsabilidades del servicio de todos los procedimientos que gestione.

#### Artículo 11. El Responsable del Sistema.

1. El Responsable del Sistema es la persona cuya responsabilidad es desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida, así

como elaborar las directrices de seguridad de tercer nivel definidas en el artículo 15 de la presente Resolución.

2. Las funciones de Responsable del Sistema recaerán en el titular de la Subdirección de Sistemas y Tecnologías de la Información y las Comunicaciones.

#### Artículo 12. Grupos de trabajo.

La CSI podrá articular la creación de grupos de trabajo para la realización de actividades que se estimen convenientes, tales como la elaboración de estudios, trabajos e informes.

#### Artículo 13. Resolución de conflictos.

En caso de conflicto entre los diferentes responsables que componen la estructura organizativa de la PSI prevalecerá la decisión de la Comisión de Seguridad de la Información.

#### Artículo 14. Gestión de los riesgos.

1. La gestión de riesgos debe realizarse de manera continua sobre el sistema de información, conforme a los principios de gestión de la seguridad basada en los riesgos y reevaluación periódica. El Responsable del Servicio es el encargado de que se realice el preceptivo análisis de riesgos y se proponga el tratamiento adecuado, calculando los riesgos residuales.

2. El Responsable de Seguridad es el encargado de recomendar un marco de directrices básicas para armonizar los criterios a seguir para la valoración de riesgos.

3. Los Responsables de la Información y del Servicio son los propietarios de los riesgos sobre la información y sobre los servicios, respectivamente, siendo responsables de su seguimiento y control, sin perjuicio de la posibilidad de delegar esta tarea.

4. El proceso de gestión de riesgos, que comprende las fases de categorización de los sistemas, análisis de riesgos y selección de medidas de seguridad a aplicar, que deberán ser proporcionales a los riesgos y estar justificadas, deberá revisarse y aprobarse cada año por el Responsable de Seguridad, a través de un Plan de Adecuación al Esquema Nacional de Seguridad.

5. Las indicadas fases del proceso de gestión de riesgos se realizarán según lo dispuesto en los anexos I y II del Real Decreto 3/2010, de 8 de enero y siguiendo las normas, instrucciones, guías CCN-STIC y recomendaciones para la aplicación

del mismo elaboradas por el Centro Criptológico Nacional, así como todo lo referente al análisis de riesgo y de impacto en la protección de datos especificado en el citado Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016.

#### Artículo 15. Desarrollo de la Política de Seguridad.

1. La Política de Seguridad de la información se desarrollará en tres niveles por ámbito de aplicación, nivel de detalle técnico y obligatoriedad de cumplimiento, de manera que cada disposición de un determinado nivel de desarrollo se fundamente en las disposiciones de nivel superior. Dichos niveles de desarrollo son los siguientes:

- a) Primer nivel: constituido por la PSI y las directrices generales de seguridad aplicables a todas las direcciones y departamentos de la Comisión Nacional de los Mercados y la Competencia.
- b) Segundo nivel: constituido por las disposiciones de seguridad desarrolladas por el Responsable de Seguridad. Estas disposiciones de seguridad deberán cumplir los siguientes requisitos:
  - i. Cumplir estrictamente con lo indicado en el ENS y con el primer nivel enunciado en el presente artículo.
  - ii. Ser aprobadas por la CSI.
- c) Tercer nivel: constituido por procedimientos, guías e instrucciones técnicas desarrollados por el Responsable del Sistema. Son documentos que, cumpliendo con lo expuesto en la PSI, determinan las acciones o tareas a realizar en el desempeño de un proceso. Este tercer nivel deberá cumplir los siguientes requisitos:
  - i. Cumplir estrictamente con lo indicado en el ENS y con el primer y segundo nivel enunciados en el presente artículo.
  - ii. Ser aprobados por el Responsable de Seguridad.

2. Además de lo señalado en el apartado 1 del presente artículo, el desarrollo de la Política de Seguridad podrá disponer de otros documentos tales como estándares de seguridad, buenas prácticas o informes técnicos.

3. Todo el personal de cada una de las direcciones y departamentos de la Comisión Nacional de los Mercados y la Competencia tendrá la obligación de conocer y cumplir, además de la presente PSI, todas las directrices generales, normas y procedimientos de seguridad de la información que puedan afectar a sus funciones.

4. La CSI establecerá los mecanismos necesarios para compartir la documentación derivada de su desarrollo con el propósito de normalizarlo, en la medida de lo posible, en todo el ámbito de aplicación de la PSI.

5. Este marco normativo estará a disposición de todos los miembros de la Comisión Nacional de los Mercados y la Competencia.

Artículo 16. Protección de datos de carácter personal.

1. En lo referente a los datos de carácter personal que sean objeto de tratamiento por parte de la Comisión Nacional de los Mercados y la Competencia, se adoptarán las medidas técnicas y organizativas que corresponda implantar atendidos los riesgos generados por el tratamiento una vez llevada a cabo la evaluación exigida por el artículo 24.1 del Reglamento (UE) 2016/679.
2. Respecto a la protección de datos de carácter personal, el Responsable del Servicio asumirá las funciones de responsable del tratamiento.
3. En caso de conflicto entre los diferentes responsables, prevalecerán las mayores exigencias derivadas de la protección de datos de carácter personal.

Artículo 17. Formación y concienciación.

1. Se desarrollarán actividades formativas específicas orientadas a la concienciación y formación de los empleados públicos de la Comisión Nacional de los Mercados y la Competencia, así como a la difusión entre los mismos de la PSI y de su desarrollo normativo.
2. El Responsable de Seguridad se encargará de promover las actividades de formación y concienciación en materia de seguridad, según lo indicado en el artículo 7, apartado 3, letra k) de esta Resolución.

Disposición adicional primera. Deber de colaboración en la implantación de la PSI.

Todas las direcciones y departamentos de la Comisión Nacional de los Mercados y la Competencia prestarán su colaboración en las actuaciones de implementación de la PSI aprobada por esta resolución.

Disposición adicional segunda. Publicidad.

Esta Resolución se publicará tanto en la sede electrónica como en la intranet de la Comisión Nacional de los Mercados y la Competencia.

Disposición adicional segunda. Revisión.

Esta PSI será revisada transcurridos 24 meses desde su publicación.

Disposición final única. Entrada en vigor.

La presente Resolución será de aplicación el día siguiente al de su publicación.

Madrid, 18 de junio de 2018

EL PRESIDENTE

José María Marín Quemada