RESOLUCIÓN DE 24 DE JUNIO DE 2024, DE LA PRESIDENCIA DE LA COMISIÓN NACIONAL DE LOS MERCADOS Y LA COMPETENCIA, POR LA QUE SE APRUEBA LA VERSIÓN CONSOLIDADA DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DE LA COMISIÓN

La Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público establece que las Administraciones Públicas se relacionarán entre sí y con sus órganos, organismos públicos y entidades vinculados o dependientes a través de medios electrónicos. Dichos medios deben asegurar la interoperabilidad y seguridad de los sistemas y soluciones adoptadas, garantizarán la protección de los datos de carácter personal y facilitarán preferentemente la prestación conjunta de servicios a los interesados. En este sentido, el artículo 156 de la citada Ley 40/2015, de 1 de octubre, regula el Esquema Nacional de Seguridad.

Por su parte, la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, recoge en su artículo 13 sobre derechos de las personas en sus relaciones con las Administraciones Públicas, el relativo a la protección de datos de carácter personal y, en particular, a la seguridad y confidencialidad de los datos que figuren en los ficheros, sistemas y aplicaciones de las Administraciones Públicas.

El Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad tiene por objeto regular el Esquema Nacional de Seguridad, establecido en el artículo 156.2 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

El ENS está constituido por los principios básicos y requisitos mínimos necesarios para una protección adecuada de la información tratada y los servicios prestados por las entidades de su ámbito de aplicación, con objeto de asegurar el acceso, la confidencialidad, la integridad, la trazabilidad, la autenticidad, la disponibilidad y la conservación de los datos, la información y los servicios utilizados por medios electrónicos que gestionen en el ejercicio de sus competencias.

Lo dispuesto en el Real Decreto 311/2022, de 3 de mayo, por cuanto afecta a los sistemas de información utilizados para la prestación de los servicios públicos, deberá considerarse comprendido en los recursos y procedimientos integrantes del Sistema de Seguridad Nacional recogidos en la Ley 36/2015, de 28 de septiembre, de Seguridad Nacional.

El documento fundamental para abordar el impulso de la normativa de seguridad de la Comisión Nacional de los Mercados y la Competencia es la Política de Seguridad de la Información, que establece los principios y directrices a tener en cuenta en su posterior desarrollo normativo y define la estructura organizativa de la seguridad de la información.

Según se establece en el capítulo III del citado Real Decreto 311/2022, de 3 de mayo, esta política de seguridad se establecerá con base en unos principios básicos (seguridad como proceso integral, gestión de la seguridad basada en riesgos, prevención, detección, respuesta y conservación,

existencia de líneas de defensa, vigilancia continua, reevaluación periódica, y diferenciación de responsabilidades) y desarrollará una serie de requisitos mínimos consignados en el artículo 12.6.

La presente Resolución, por tanto, tiene la finalidad de aprobar la versión actualizada de la Política de Seguridad de la Información de la Comisión Nacional de los Mercados y la Competencia, para un mejor alineamiento con lo dispuesto en el ENS y efectuar otras oportunas rectificaciones en el documento, dejando sin efecto la anteriormente vigente por resolución de la presidencia el 13 de febrero de 2024.

En virtud de lo anterior y en cumplimiento del artículo 12 del Real Decreto 311/2022, de 3 de mayo, la Presidenta de la Comisión Nacional de los Mercados y la Competencia, en uso de las facultades que legal y reglamentariamente tiene atribuidas, resuelve:

Artículo 1. Objeto y ámbito de aplicación.

1. Constituye el objeto de la presente resolución la aprobación de la Política de Seguridad de la Información (en adelante PSI) de los sistemas de información de la Comisión Nacional de los Mercados y la Competencia, así como del marco organizativo y tecnológico de la misma.

2. La PSI será de obligado cumplimiento para todas las direcciones y departamentos de la Comisión Nacional de los Mercados y la Competencia.

3. La PSI será de obligado cumplimiento para todo el personal que acceda tanto a los sistemas de información como a la propia información que sea gestionada por la Comisión Nacional de los Mercados y la Competencia, con independencia de cuál sea su destino, adscripción o relación con la misma.

Artículo 2. Misión del Organismo

La Comisión Nacional de los Mercados y la Competencia tiene por objeto garantizar, preservar y promover el correcto funcionamiento, la transparencia y la existencia de una competencia efectiva en todos los mercados y sectores productivos, en beneficio de los consumidores y usuarios.

Artículo 3. Marco legal y regulatorio

El marco normativo en el que la Comisión Nacional de los Mercados y la Competencia desarrolla sus actividades está regulado, esencialmente, por las siguientes disposiciones:

a) Ley 3/2013, de 4 de junio, de creación de la Comisión Nacional de los Mercados y de la Competencia.

b) Real Decreto 657/2013, de 30 de agosto, por el que se aprueba el Estatuto Orgánico de la CNMC.

c) Ley 15/2007, de 3 de julio, de Defensa de la Competencia.

d) Ley 11/2022, de 28 de junio, General de Telecomunicaciones.

e) Ley 13/2022, de 7 de julio, General de Comunicación Audiovisual.

f) Ley 24/2013, de 26 de diciembre, del Sector Eléctrico.

g) Ley 34/1998, de 7 de octubre, del Sector de Hidrocarburos.

h) Ley 38/2015, de 29 de septiembre, del Sector Ferroviario.

i) Ley 43/2010, de 30 de diciembre, del Servicio Postal Universal, de los derechos de los usuarios.

j) Ley 20/2013, de 9 de diciembre, de Garantía de la Unidad de Mercado.

En sus actuaciones, la CNMC se rige asimismo por la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, y la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

Artículo 4. Principios de la seguridad de la información.

1. Los principios básicos son directrices fundamentales de seguridad que han de tenerse siempre presentes en cualquier actividad relacionada con el uso de los activos de información. Se establecen los siguientes:

a) Alcance estratégico: La seguridad de la información debe contar con el compromiso y apoyo de todos los niveles directivos de forma que pueda estar coordinada e integrada con el resto de iniciativas estratégicas de la Comisión Nacional de los Mercados y la Competencia para conformar un todo coherente y eficaz.

b) Diferenciación de responsabilidades: En los sistemas de información se diferenciará el responsable de la información, que determina los requisitos de seguridad de la información tratada; el responsable del servicio, que determina los requisitos de seguridad de los servicios prestados; el responsable del sistema, que tiene la responsabilidad sobre la prestación de los servicios y el responsable de seguridad, que determina las decisiones para satisfacer los requisitos de seguridad de la información y los servicios.

c) Seguridad como proceso integral: La seguridad se entenderá como un proceso integral constituido por todos los elementos técnicos, humanos, materiales, jurídicos y organizativos, relacionados con el sistema, evitando, salvo casos de urgencia o necesidad, cualquier actuación puntual o tratamiento coyuntural. La seguridad de la información debe considerarse como parte de la operativa habitual, estando presente y aplicándose desde el diseño inicial de los sistemas de información.

d) Gestión de la seguridad basada en Riesgos: El análisis y gestión de riesgos será parte esencial del proceso de seguridad. La gestión de riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. La reducción de estos niveles se realizará mediante el despliegue de medidas de seguridad, que establecerá un

equilibrio entre la naturaleza de los datos y los tratamientos, el impacto y la probabilidad de los riesgos a los que estén expuestos y la eficacia y el coste de las medidas de seguridad. Al evaluar el riesgo en relación con la seguridad de los datos, se deben tener en cuenta los riesgos que se derivan del tratamiento de los datos personales.

e) Proporcionalidad: El establecimiento de medidas de protección, detección y recuperación deberá ser proporcional a los potenciales riesgos y a la criticidad y valor de la información y de los servicios afectados.

f) Mejora continua: Las medidas de seguridad se reevaluarán y actualizarán periódicamente para adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección. La seguridad de la información será atendida, revisada y auditada por personal cualificado, instruido y dedicado.

g) Seguridad por defecto: Los sistemas deben diseñarse y configurarse de forma que garanticen un grado suficiente de seguridad por defecto.

h) Prevención, detección, respuesta y conservación: Las medidas de prevención deben eliminar o, al menos reducir, la posibilidad de que las amenazas lleguen a materializarse. Estas medidas de prevención contemplarán, entre otras, la disuasión y la reducción de la exposición. Las medidas de detección irán dirigidas a descubrir la presencia de un ciberincidente y estarán acompañadas de medidas de respuesta, de forma que los incidentes de seguridad se atajen a tiempo. Las medidas de recuperación permitirán la restauración de la información y los servicios. El sistema de información garantizará la conservación de los datos e información en soporte electrónico.

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. 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 Seguridad.

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.

k) Profesionalidad: La seguridad de los sistemas de información estará atendida y será revisada y auditada por personal cualificado, dedicado e instruido en todas las fases de su ciclo de vida. La CNMC exigirá, 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 y deberán designar un POC (Punto o Persona de Contacto) para la seguridad de la información tratada y el servicio prestado.

l) Mínimo privilegio: Los sistemas de información se diseñarán y configurarán otorgando sólo los permisos y privilegios necesarios de forma que los usuarios o procesos solo tengan acceso a los recursos que necesitan para cumplir con su función específica, y no tengan acceso a ningún otro recurso ni privilegios innecesarios.

m) Integridad y actualización del sistema: cualquier elemento físico o lógico en el catálogo actualizado de activos del sistema, o su modificación, requerirá autorización formal previa. La evaluación y monitorización permanentes permitirán adecuar el estado de seguridad de los sistemas atendiendo a las deficiencias de configuración, las vulnerabilidades identificadas y las actualizaciones que les afecten y la detección temprana de cualquier incidente que tenga lugar sobre los mismos.

n) Protección de información almacenada y en tránsito: se prestará especial atención a la información almacenada o en tránsito a través de los equipos o dispositivos portátiles o móviles, los dispositivos periféricos, los soportes de información y las comunicaciones sobre redes abiertas, que deberán analizarse especialmente para lograr una adecuada protección. Se aplicarán procedimientos que garanticen la recuperación y conservación a largo plazo de los documentos electrónicos. Toda información en soporte no electrónico que haya sido causa o consecuencia directa de la información electrónica deberá estar protegida con el mismo grado de seguridad que ésta.

o) Prevención ante otros sistemas de información interconectados: Se protegerá el perímetro del sistema de información reforzándose las tareas de prevención, detección y respuesta a incidentes de seguridad.

p) Registro de actividad y detección de código dañino: Al objeto de preservar la seguridad de los sistemas de información, con plenas garantías legales y de acuerdo con la normativa sobre protección de datos personales, se registrarán las actividades de los usuarios, reteniendo la información estrictamente necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa. El registro de actividad será únicamente para los fines de seguridad de la información, de forma que sea posible impedir el acceso no autorizado a las redes y sistemas de información, detener los ataques de denegación de servicio, evitar la distribución malintencionada de código dañino, así como otros daños a las antedichas redes y sistemas de información.

q) Continuidad de las operaciones: Se dispondrán de copias de seguridad y se establecerán los mecanismos necesarios para garantizar la continuidad de las operaciones en caso de pérdida de los medios habituales.

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.

3. En caso de que la función de Responsable de Seguridad y de Responsable del Sistema recaiga en la misma persona o en distintas personas entre las que exista relación jerárquica, deberán aplicarse medidas compensatorias para garantizar la finalidad del principio de diferenciación de responsabilidades previsto en el artículo 11 del ENS.

4. Tanto los miembros de la Comisión de Seguridad de la Información, como el resto de responsables de la estructura organizativa de seguridad serán renovados con ocasión de vacante.

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:

a) Presidente: El titular de la Secretaría General. Tendrá voto de calidad en la toma de decisiones del Comité.

b) Vicepresidente: El titular de la Subdirección de Sistemas y Tecnologías de la Información y las Comunicaciones.

c) Vocales: Un representante de cada una de las siguientes direcciones o departamentos. Serán nombrados por la Presidenta 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 de la Presidenta

   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.

d) Secretario: un empleado público de grupo 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 la Presidenta 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 la Presidenta 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 a la Presidenta 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. La Presidenta 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 normas 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 311/2022, de 3 de mayo 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 311/2022, de 3 de mayo, 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 citato 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 citato 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 disposiciones 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 responsables de la gestión 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 311/2022, de 3 de mayo 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 citato 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 de la Comisión Nacional de los Mercados y la Competencia.

b) Segundo nivel: constituido por las normas de seguridad desarrolladas por el Responsable de Seguridad. Estas normas 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 tercera. Revisión.

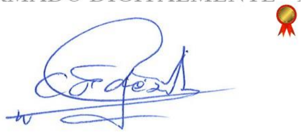
Esta PSI será revisada transcurridos 24 meses desde su publicación.

Disposición final única. Entrada en vigor.

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

Madrid, a fecha de la firma electrónica

LA PRESIDENTA



Doña Cani Fernández Vicién