Orden de 31 de julio de 2013, de la Consejería de Presidencia, Justicia e Igualdad, por la que se establece el marco común y las directrices básicas de la política de seguridad de la información en el ámbito de la Administración Electrónica de la Administración Pública de la Comunidad Autónoma de Canarias *(BOC 153. de 9.7.2013)* (1)

La Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, señala entre sus fines el crear las condiciones de confianza en el uso de los medios electrónicos, estableciendo las medidas necesarias para la preservación de la integridad de los derechos fundamentales, y en especial los relacionados con la intimidad y la protección de datos de carácter personal, por medio de la garantía de la seguridad de los sistemas, los datos, las comunicaciones y los servicios electrónicos. Estos fines han sido desarrollados por 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).

El citado Real Decreto 3/2010, de 8 de enero, persigue fundamentar la confianza en que los sistemas de información prestarán sus servicios y custodiarán la información de acuerdo con sus especificaciones funcionales, sin interrupciones o modificaciones fuera de control, y sin que la información pueda llegar a conocimiento de personas no autorizadas.

El ENS establece el marco regulatorio de la Política de Seguridad de la Información (PSI), que se plasma en un documento, accesible y comprensible para todos los miembros, que define lo que significa seguridad de la información en una organización determinada y que rige la forma en que una organización gestiona y protege la información y los servicios que considera críticos.

Por su parte la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y sus normas de desarrollo aportan criterios para establecer la proporcionalidad entre las medidas de seguridad y la información a proteger.

En el ámbito de la Comunidad Autónoma de Canarias el Decreto 19/2011, de 10 de febrero, por el que se regula la utilización de los medios electrónicos en la Administración Pública de la Comunidad Autónoma de Canarias (2), garantiza, en el marco de los principios y derechos reconocidos en la Ley 11/2007, la igualdad, autenticidad, integridad, disponibilidad, accesibilidad, confidencialidad y conservación de la información y de los documentos electrónicos, así como la protección de datos de carácter personal. A tal fin prevé en su Disposición Adicional Cuarta la aprobación, previo informe de la Comisión Superior de Tecnologías de la Información, de la política de seguridad que se ha de aplicar en la utilización de los medios electrónicos.

La presente Orden establece el compromiso de la Administración Pública de la Comunidad Autónoma de Canarias con la seguridad de los sistemas de la información, define los objetivos y criterios básicos para el tratamiento de la misma, sienta las bases del marco normativo de seguridad de esta administración y la estructura mínima organizativa y de gestión que velará por su cumplimiento.

Por cuanto antecede, visto el informe de la Comisión Superior de Tecnologías de la Información de fecha 5 de junio de 2012, y en el ejercicio de las competencias que me atribuye *el artículo 23.a) del Decreto 331/2011, de 22 de diciembre, por el que se aprueba el Reglamento Orgánico de la Consejería de Presidencia, Justicia e Igualdad* (3) y la Disposición Adicional Cuarta del Decreto 19/2011, de 10 de febrero, por el que se regula la utilización de los medios electrónicos en la Administración Pública de la Comunidad Autónoma de Canarias (2),

DISPONGO:

CAPÍTULO PRIMERO

Disposiciones generales

Artículo 1. Objeto y ámbito de aplicación.

1. La presente Orden tiene por objeto establecer el marco común y las directrices básicas de las políticas de seguridad de la información (en adelante, PSI) en el ámbito de la Administración Electrónica de la Administración Pública de la Comunidad Autónoma de Canarias, así como el establecimiento del marco básico organizativo y tecnológico de las mismas.

2. Esta Orden será de aplicación a las PSI que en el ámbito de la Administración Electrónica de la Administración Pública de la Comunidad Autónoma de Canarias se aprueben por los distintos departamentos, entidades de derecho público y organismos autónomos, siendo de aplicación a todos sus sistemas de información y debiendo ser observada por todo el personal de los mismos, así como

(1) La presente Orden se transcribe con las modificaciones introducidas por Orden de 15 de diciembre de 2016 (BOC 246, de 22.12.2016).

(2) El Decreto 19/2011 figura como D19/2011.

(3) Derogado. Esta referencia debe entenderse realizada al artículo 27 del Decreto 382/2015, de 28 de diciembre, por el que se aprueba el Reglamento Orgánico de la Consejería de Presidencia, Justicia e Igualdad (D382/2015).

por aquellas personas que, no perteneciendo a su organización, tengan acceso a sus sistemas de información o a la información gestionada por ellos.

Artículo 2. Políticas de seguridad de la información (PSI).

1. Sin perjuicio de las directrices establecidas en la presente Orden, cada organismo incluido en su ámbito de aplicación deberá desarrollar y aprobar el documento de PSI en el ámbito de la administración electrónica del organismo, así como las normas y procedimientos que adecuen, en su caso, el marco común y las directrices básicas en la Administración Pública de la Comunidad Autónoma de Canarias a sus particularidades.

En cualquier caso, las normas y procedimientos organizativos que se desarrollen a partir de cada PSI, deberán respetar y cumplir aquellas normas, procedimientos y medidas de seguridad corporativas que sean aprobadas por el órgano con competencias en materia de telecomunicaciones y sistemas de información, actuando aquellas como directrices complementarias.

2. La PSI en el ámbito de la Administración Electrónica de cada departamento, entidad de derecho público y organismo autónomo deberá ser aprobada mediante orden del titular de la consejería correspondiente o resolución del órgano competente de la entidad pública u organismo autónomo, que deberá publicarse en el Boletín Oficial de Canarias (1).

No obstante lo anterior, por razones técnicas, de economía o de eficacia, la PSI de cada departamento podrá incluir la de sus entidades de derecho público y organismos autónomos dependientes.

3. La aprobación de las PSI requerirá informe previo del órgano competente en materia de tecnologías de la información y la comunicación, que versará sobre el cumplimiento del marco común y directrices básicas establecidas en la presente Orden.

4. Las PSI de los sistemas de información corporativos serán aprobadas por orden del titular de la consejería competente en la materia a la que se refiere la información tratada en cada sistema (2).

Artículo 3. Misión de la organización.

Las PSI deberán hacer referencia a la misión del departamento, entidad de derecho público u organismo autónomo correspondiente.

Artículo 4. Objetivos del marco común y las directrices básicas de la PSI.

El marco común y las directrices básicas de las PSI en el ámbito de la Administración Electrónica de la Administración Pública de la Comunidad Autónoma de Canarias persiguen la consecución de los siguientes objetivos:

a) Garantizar a toda la ciudadanía que sus datos serán gestionados de acuerdo a los estándares y buenas prácticas en seguridad de las tecnologías de la información y la comunicación (en adelante, TIC).

b) Aumentar el nivel de concienciación en materia de seguridad TIC de todos los organismos a los que es de aplicación la presente Orden, garantizando que el personal a su servicio es consciente de sus obligaciones y responsabilidades.

c) Establecer las bases de un modelo común de gestión de la seguridad TIC en la Administración Pública de la Comunidad Autónoma de Canarias, que cubra en un ciclo continuo de mejora los aspectos técnicos, organizativos y procedimentales.

d) Garantizar el cumplimiento de la legislación vigente en materia de seguridad TIC.

Artículo 5 Principios de las PSI.

Sin perjuicio de los principios básicos establecidos en el Esquema Nacional de Seguridad, las políticas de seguridad en el ámbito de la Administración Electrónica de la Administración Pública de la Comunidad Autónoma de Canarias se desarrollarán, con carácter general, de acuerdo a los siguientes principios:

a) Principio de confidencialidad: los sistemas de información deberán ser accesibles únicamente para aquellas personas usuarias, órganos y entidades o procesos expresamente autorizados para ello, con respeto a las obligaciones de secreto y sigilo profesional.

b) Principio de integridad y calidad: se deberá garantizar el mantenimiento de la integridad y calidad de la información, así como de los procesos de tratamiento de la misma, estableciéndose los mecanismos para asegurar que los procesos de creación, tratamiento, almacenamiento y distribución de la información contribuyen a preservar su exactitud y corrección.

c) Principio de disponibilidad y continuidad: se garantizará un alto nivel de disponibilidad en los sistemas de información y se dotarán de los planes y medidas necesarias para asegurar la continuidad de los servicios y la recuperación ante posibles contingencias graves.

d) Principio de gestión del riesgo: se deberá articular un proceso continuo de análisis y trata-

(1) Véase Decreto 160/2009, de 21 de diciembre, por el que se aprueba el Reglamento del Boletín Oficial de Canarias (BOC) (D160/2009).

(2) El apartado 4 del artículo 2 se transcribe con la nueva redacción dada por Orden de 15 de diciembre de 2016 (BOC 246, de 22.12.2016).

miento de riesgos como mecanismo básico sobre el que debe descansar la gestión de la seguridad de los sistemas de información.

e) Principio de proporcionalidad en coste: la implantación de medidas que mitiguen los riesgos de seguridad de los sistemas de información deberá hacerse bajo un enfoque de proporcionalidad en los costes económicos y operativos.

f) Principio de concienciación y formación: se articularán iniciativas que permitan a las personas usuarias conocer sus deberes y obligaciones en cuanto al tratamiento seguro de la información. De igual forma, se fomentará la formación específica en materia de seguridad TIC de todas aquellas personas que gestionan y administran sistemas de información y telecomunicaciones.

g) Principio de prevención: se desarrollarán planes y líneas de trabajo específicas orientadas a prevenir fraudes, incumplimientos o incidentes relacionados con la seguridad TIC.

h) Principio de mejora continua: se revisará el grado de eficacia de los controles de seguridad TIC implantados, al objeto de adecuarlos a la constante evolución de los riesgos y del entorno tecnológico de la Administración Pública de la Comunidad Autónoma de Canarias.

i) Principio de seguridad TIC en el ciclo de vida de los sistemas de información: las especificaciones de seguridad se incluirán en todas las fases del ciclo de vida de los servicios y sistemas, acompañadas de los correspondientes procedimientos de control.

j) Principio de función diferenciada: la responsabilidad de la seguridad de los sistemas de información estará diferenciada de la responsabilidad sobre la prestación de los servicios.

Artículo 6. Definiciones.

Los términos, palabras, expresiones y las definiciones contenidas en la presente Orden han de ser entendidas en el siguiente sentido:

Gestión de riesgos: Actividades coordinadas para dirigir y controlar una organización con respecto a los riesgos.

Misión de la organización: Razón de la existencia de la organización, el propósito básico hacia el que apuntan las actividades y servicios que presta.

Política de seguridad: Conjunto de directrices plasmadas en documento escrito, que rigen la forma en que una organización gestiona y protege la información y los servicios que considera críticos.

Riesgo: Estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización.

Sistema de Información: 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.

Sistemas de información corporativos: aquellos sistemas de información cuyo ámbito de aplicación y uso es general y común para toda la Administración Pública de la Comunidad Autónoma de Canarias.

CAPÍTULO II

Organización de las PSI

Artículo 7. Responsabilidad general.

La preservación de la seguridad TIC en el ámbito de la Administración Electrónica será considerada objetivo común de todas las personas al servicio de la Administración Pública de la Comunidad Autónoma de Canarias, siendo estas responsables del uso correcto de los sistemas de información puestos a su disposición.

Artículo 8. Responsable de la Coordinación en Seguridad TIC de la Administración Pública de la Comunidad Autónoma de Canarias.

1. El órgano competente en materia de tecnologías de la información y la comunicación será responsable de la coordinación en materia de seguridad TIC en el ámbito de la Administración Electrónica.

2. En el ejercicio de dicha atribución, tendrá las siguientes funciones:

a) Emisión del informe previsto en el apartado 3 del artículo 2 de la presente Orden.

b) Asesorar a los distintos departamentos, entes públicos y organismos en la elaboración de su PSI.

c) Elevar propuestas e informes a la Comisión Superior de Tecnologías de la Información.

Artículo 9. Estructura organizativa de las PSI.

Las estructuras organizativas de la gestión de las PSI en el ámbito de la Administración Electrónica estarán compuestas, como mínimo, por:

a) El Comité para la Gestión y Coordinación de la Seguridad de la Información.

b) Los Responsables de la Información.

c) Los Responsables del Servicio.

d) Los Responsables de Seguridad.

e) Los Responsables del Sistema.

Artículo 10. Comité para la Gestión y Coordinación de la Seguridad de la Información.

1. El Comité para la Gestión y Coordinación de la Seguridad de la Información (en adelante, el Comité) se creará como un grupo de trabajo en el seno del departamento, entidad de derecho público u organismo público correspondiente.

2. El Comité tendrá, como mínimo, la siguiente composición:

a) Presidencia: la persona designada como responsable de seguridad (1).

b) Vocalías: personas titulares de Direcciones Generales o asimiladas.

c) Secretaría: una persona con vínculo funcionarial del departamento, entidad de derecho público u organismo autónomo designado por la Presidencia, que actuará con voz y sin voto.

3. El Comité coordinará todas las actividades relacionadas con la seguridad de los sistemas de información y ejercerá, como mínimo, las siguientes funciones:

a) Elaborar los borradores de modificación y actualización de la PSI.

b) Analizar los riesgos e impulsar su evaluación.

c) Impulsar la actualización de los criterios y directrices sobre seguridad de la información.

d) Impulsar medidas para mejorar y reforzar los sistemas de seguridad y control.

e) Impulsar el cumplimiento y difusión de la PSI, promoviendo las actividades de concienciación y formación en materia de seguridad para el personal del departamento, entidad de derecho público u organismo autónomo.

f) Elaborar los borradores de directrices y normas de seguridad generales para todo el departamento, entidad de derecho público u organismo autónomo que deberá cumplir el marco normativo indicado en el artículo 18 de la presente Orden.

g) Elaborar la normativa de seguridad de segundo nivel, que según el artículo 18 de la presente Orden, se corresponde con las políticas específicas de seguridad y con las Normas de Seguridad TIC (en adelante, Normas STIC), de obligado cumplimiento.

h) Coordinar las decisiones y actuaciones de los diferentes Responsables de Seguridad, asesorando la resolución de los posibles conflictos entre los mismos bajo el criterio de garantizar la seguridad de las infraestructuras tecnológicas compartidas.

i) Impulsar los proyectos para la adecuación al cumplimiento del Esquema Nacional de Seguridad.

j) Compartir experiencias de éxito en materia de seguridad entre sus miembros para velar por el cumplimiento de la PSI y su normativa de desarrollo.

4. El Comité ajustará su funcionamiento a las previsiones contenidas en el capítulo II del Título II de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

5. El Comité se deberá reunir con carácter ordinario al menos una vez al año, y con carácter extraordinario cuando lo decida su Presidencia. Las reuniones se realizarán en horario de trabajo y, cuando proceda, por videoconferencia. No se percibirán indemnizaciones en concepto de asistencia por concurrencia al Comité.

6. El Comité podrá recabar de personal técnico la información o asesoramiento pertinente para el ejercicio de sus funciones. En caso necesario este personal podrá ser convocado por el Comité para su asistencia a las reuniones, en calidad de asesores, con voz pero sin voto.

7. Podrá acordarse la constitución de subgrupos de trabajo para el análisis, elaboración y ejecución de trabajos o actividades específicas, dentro del ámbito de sus funciones.

Artículo 11. Los Responsables de la Información.

1. Conforme a los artículos 10 y 44 del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (ENS), el Responsable de la Información es la persona que establece las necesidades de seguridad de la información que se maneja y efectúa las valoraciones del impacto que tendría un incidente que afectara a su seguridad. Tiene además, en exclusiva, la potestad de modificar el nivel de seguridad requerido para la misma (anexo II.5.7.2 del ENS).

2. Esta responsabilidad recaerá en el titular del órgano que gestione cada procedimiento o trámite.

3. Son funciones de cada Responsable de Información, dentro de su ámbito de actuación, las siguientes:

a) Determinar los niveles de seguridad de la información tratada, valorando los impactos de los incidentes que afecten a la seguridad de la información (artículo 44 del ENS).

b) Son los responsables, junto a los Responsables del Servicio, de aceptar los riesgos residuales calculados en el análisis de riesgos, y de realizar su seguimiento y control.

Artículo 12. Los Responsables del Servicio.

1. Conforme al artículo 10 del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (ENS) el Responsable

(1) La letra a) del apartado 2 del artículo 10 se transcribe con la nueva redacción dada por Orden de 15 de diciembre de 2016 (BOC 246, de 22.12.2016).

del Servicio es la persona que determina los requisitos de seguridad de los servicios prestados.

2. Esta responsabilidad recaerá en el titular del órgano que gestione cada servicio.

3. Respecto al proceso de gestión del riesgo, los Responsables del Servicio son los encargados, junto a los Responsables de la Información, de aceptar los riesgos residuales calculados en el análisis de riesgos, y de realizar su seguimiento y control.

Artículo 13 Los Responsables de Seguridad.

1. Conforme al artículo 10 del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (ENS), el Responsable de Seguridad es la persona que determina las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios.

2. Esta responsabilidad recaerá en la persona titular del órgano administrativo que designe el titular del departamento u órgano equivalente del ente público u organismo autónomo y no podrá recaer en la persona responsable del sistema (1).

3. Serán funciones de cada Responsable de Seguridad, como mínimo, las siguientes:

a) Promover la seguridad de la información manejada y de los servicios electrónicos prestados por los sistemas de información.

b) Proponer la normativa de seguridad de segundo nivel, que según el artículo 18 de la presente orden, se corresponde con las políticas específicas de seguridad y con las normas STIC, de obligado cumplimiento.

c) Aprobar la normativa de seguridad de tercer nivel, que según el artículo 18 de la presente orden, se corresponde a los procesos, procedimientos STIC e instrucciones técnicas STIC.

d) Procurar que la documentación de seguridad se mantenga organizada y actualizada, y de gestionar los mecanismos de acceso a la misma.

e) Promover las actividades de concienciación y formación en materia de seguridad en su ámbito de responsabilidad.

f) Realizar la coordinación y seguimiento de la implantación de los proyectos de adecuación al Esquema Nacional de Seguridad.

g) Realizar los preceptivos análisis de riesgos, de seleccionar las salvaguardas a implantar y de revisar el proceso de gestión del riesgo, elevando un informe anual al Comité.

h) Promover auditorías periódicas para verificar el cumplimiento de las obligaciones en materia de seguridad de la información, y analizar los informes de auditoría, elaborando las conclusiones a presentar a los Responsables del Servicio y los Responsables de la Información para que adopten las medidas correctoras adecuadas.

i) Coordinar el proceso de Gestión de la Seguridad.

j) Firmar la Declaración de Aplicabilidad, que comprende la relación de medidas de seguridad seleccionadas para un sistema (artº. 27 y anexo II.2 del ENS).

k) Elaborar informes periódicos de seguridad que incluyan los incidentes más relevantes de cada período.

l) Determinar 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.

4. Cuando la complejidad, distribución, separación física de sus elementos o número de usuarios de los sistemas de información lo justifiquen, cada Responsable de Seguridad podrá designar los responsables de seguridad delegados que considere necesarios, que tendrán dependencia funcional directa de aquel y serán responsables en su ámbito de todas aquellas acciones que les delegue el mismo.

5. Para el ejercicio de sus funciones podrá contar con el asesoramiento y apoyo del Comité para la Gestión y Coordinación de la Seguridad de la Información.

Artículo 14. Los Responsables del Sistema.

1. Esta responsabilidad recaerá en los titulares de los órganos responsables del desarrollo, mantenimiento y explotación del sistema de información que soporte los servicios correspondientes.

2. Las funciones de los Responsables del Sistema serán las siguientes:

a) Implantar las medidas necesarias para garantizar la seguridad del sistema durante todo su ciclo de vida, siguiendo las indicaciones del Responsable de Seguridad.

b) Aprobar toda modificación sustancial de la configuración de cualquier elemento del sistema.

c) Suspender el manejo de una determinada información o la prestación de un servicio electrónico si es informado de deficiencias graves de seguridad, previo acuerdo con el Responsable de dicha información o servicio, y con el Responsable de Seguridad.

3. Las funciones citadas en el punto anterior podrán recaer en diferentes personas, en el caso

(1) El apartado 2 del artículo 13 se transcribe con la nueva redacción dada por Orden de 15 de diciembre de 2016 (BOC 246, de 22.12.2016).

de que las competencias sobre los diferentes activos que componen el sistema (aplicaciones, redes, etc.) o las diferentes fases del ciclo de vida del sistema recaigan sobre órganos distintos.

Artículo 15. Resolución de conflictos.

1. En caso de conflicto entre los diferentes responsables que componen la estructura organizativa de una PSI, este será resuelto por el superior jerárquico de los mismos. En su defecto, será resuelto por el titular del departamento u órgano equivalente de la entidad de derecho público u organismo autónomo, oído el Comité para la Gestión y Coordinación de la Seguridad de la Información.

2. En caso de conflictos entre los responsables que componen la estructura organizativa de una PSI y los definidos en seguimiento de la normativa de protección de datos de carácter personal, prevalecerá la decisión que determine el responsable del fichero que presente un mayor nivel de exigencia respecto a la protección de los datos de carácter personal.

Artículo 16. Obligaciones del personal.

1. Todo el personal que presta servicios en los departamentos, entidades de derecho público y organismos autónomos, tiene la obligación de conocer y cumplir su Política de Seguridad de la Información y la normativa de seguridad derivada, siendo responsabilidad del Comité disponer los medios necesarios para que la información llegue a los afectados.

2. Todo el personal que se incorpore a uno de dichos organismos o vaya a tener acceso a alguno de sus sistemas de información o la información gestionada por ellos deberá ser informado de la PSI.

Artículo 17. Gestión de riesgos.

1. Todos los departamentos, entidades de derecho público y organismos autónomos deberán contemplar la gestión de riesgos dentro de su PSI.

2. 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 (artículo 6 del Real Decreto 3/2010, de 8 de enero) y reevaluación periódica (artículo 9 del Real Decreto 3/2010, de 8 de enero).

3. Los Responsables de Seguridad son los encargados de realizar los preceptivos análisis de riesgos, y de seleccionar las salvaguardas a implantar.

4. Los Responsables de la Información y del Servicio son los responsables de los riesgos sobre la información y sobre los servicios, respectivamente, y por tanto de aceptar los riesgos residuales calculados en el análisis, y de realizar su seguimiento y control.

5. 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 cada año por parte del Responsable de Seguridad, que elevará un informe al Comité para la Gestión y Coordinación de la Seguridad de la Información.

Artículo 18. Marco normativo de las PSI. Documentación de Seguridad.

1. Las PSI deberán recoger el marco normativo en el que se desarrollan las actividades del departamento, entidad de derecho público u organismo autónomo, que comprenderá la legislación sectorial reguladora de la actuación de los órganos de dichas entidades, así como la normativa en vigor correspondiente a la Administración Electrónica.

2. También formarán parte del marco normativo las restantes normas aplicables a la Administración Electrónica del departamento, entidad de derecho público u organismo autónomo derivadas de las anteriores y publicadas en las sedes electrónicas comprendidas dentro del ámbito de aplicación de la PSI.

3. Todas las PSI deberán contener un cuerpo normativo sobre seguridad de la información que será de obligado cumplimiento y se desarrollará en tres niveles, según el ámbito de aplicación y nivel de detalle técnico, de manera que cada norma de un determinado nivel de desarrollo se fundamente en las normas de nivel superior. Dichos niveles de desarrollo normativo son los siguientes:

a) Primer nivel normativo: la presente Orden, la disposición normativa que apruebe la Política de Seguridad de la Información, y directrices y normas de seguridad generales para todo departamento, entidad de derecho público u organismo autónomo.

b) Segundo nivel normativo: Políticas Específicas de Seguridad de la Información y Normas de Seguridad TIC (Normas STIC). Las Políticas Específicas desarrollan con un mayor grado de detalle la PSI dentro de un ámbito determinado. Las Normas dan respuesta, sin entrar en detalles de implementación ni tecnológicos, a qué se puede hacer y qué no en relación a un cierto tema desde el punto de vista de la seguridad: qué se considera un uso apropiado o inapropiado, las consecuencias derivadas del incumplimiento, entre otros aspectos.

Los documentos relativos a este segundo nivel normativo los deberá elaborar el Comité para la Gestión y Coordinación de la Seguridad de la Información. Serán aprobados, a propuesta del Respon-

sable de Seguridad, por el titular del departamento u órgano equivalente de la entidad de derecho público u organismo autónomo correspondiente.

c) Tercer nivel normativo: Procesos y Procedimientos STIC e Instrucciones Técnicas STIC. Son documentos que dan respuesta, incluyendo detalles de implementación y tecnológicos, a cómo se puede realizar una determinada tarea respetando los principios de seguridad de la organización, y los procesos internos en ella establecidos.

Los Procesos, Procedimientos STIC e Instrucciones Técnicas STIC serán aprobados por el Responsable de Seguridad.

4. Aparte de los documentos citados en el apartado 1, la documentación de seguridad del sistema podrá contar, bajo criterio del Responsable de Seguridad, con otros documentos de carácter no vinculante: recomendaciones, buenas prácticas, informes, registros, evidencias electrónicas, entre otros aspectos.

5. Los Responsables de Seguridad serán responsables de mantener la documentación de seguridad actualizada y organizada, y de gestionar los mecanismos de acceso a la misma.

6. El Comité establecerá los mecanismos necesarios para compartir la documentación derivada del desarrollo normativo con el propósito de normalizarlo, en la medida de lo posible, en todo el ámbito de aplicación de la PSI.

Artículo 19 Protección de datos de carácter personal.

1. En lo que se refiere a los ficheros con datos de carácter personal, estarán referenciados en el correspondiente Documento de Seguridad donde se hará constar tanto los ficheros afectados como los responsables correspondientes.

2. Todos los sistemas de información de la Administración Pública de la Comunidad Autónoma de Canarias se ajustarán a los niveles de seguridad requeridos por la normativa de protección de datos de carácter personal. En caso de conflicto con la normativa de seguridad indicada en el artículo anterior, prevalecerá la norma que presente un mayor nivel de exigencia respecto a la protección de los datos de carácter personal.

Artículo 20. Formación y concienciación.

1. Todos los departamentos, entidades de derecho público y organismos autónomos deberán desarrollar actividades formativas específicas orientadas a la concienciación y formación de sus empleados públicos, así como a la difusión entre los mismos de la PSI y de su desarrollo normativo.

2. Los Comités para la Gestión y Coordinación de la Seguridad de la Información y los Responsables de Seguridad se encargarán de promover las actividades de formación y concienciación en materia de seguridad, según lo indicado en el artículo 10, apartado 3, letra e) y en el artículo 13, apartado 3, letra e) de la presente Orden.

Artículo 21. Actualización de las PSI.

Las propuestas de revisión de las PSI las elaborarán los Responsables de Seguridad con el apoyo del Comité para la Gestión y Coordinación de la Seguridad de la Información y serán aprobadas por el titular del departamento u órgano equivalente de la entidad de derecho público u organismo autónomo.

Disposición Adicional Única.

La aplicación de las previsiones contenidas en esta Orden no supondrá incremento del gasto público. Por tanto, los órganos y entidades afectadas deberán desarrollar las medidas derivadas de su cumplimiento ateniéndose a sus disponibilidades presupuestarias ordinarias, no dando lugar, en ningún caso, a planteamientos de necesidades adicionales de financiación.

Disposición Derogatoria Única.

Quedan derogadas cuantas disposiciones de igual o inferior rango que se opongan a la presente Orden.

Disposiciones Finales.

Primera. Facultad para dictar instrucciones de interpretación y aplicación.

Se faculta a la Inspección General de Servicios y a la Dirección General de Telecomunicaciones y Nuevas Tecnologías, para dictar las instrucciones que sean necesarias para la correcta interpretación y aplicación de la presente orden.

Segunda. Entrada en vigor.

La presente orden entrará en vigor el día siguiente al de su publicación en el Boletín Oficial de Canarias.