3. Otras disposiciones

CONSEJERÍA DE JUSTICIA E INTERIOR

ORDEN de 22 de diciembre de 2014, por la que se establece la política de la seguridad de la información en el ámbito de la Administración Electrónica de la Consejería de Justicia e Interior, así como el marco organizativo y tecnológico.

En aras de ofrecer a la ciudadanía las condiciones de confianza necesarias en el uso de los medios electrónicos, se pretenden establecer 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. En relación con lo anterior, la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, indica que es preciso garantizar la seguridad de los sistemas de información, de las comunicaciones y de los datos y servicios por ellos manejados.

En el ámbito de la Administración Electrónica se entiende por seguridad la capacidad de las redes o de los sistemas de información para resistir, con un determinado nivel de confianza, los accidentes y las acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad, confidencialidad y trazabilidad de los datos almacenados o transmitidos y de los servicios que dichas redes o sistemas ofrecen, o a través de los cuales se realiza el acceso.

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, 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 Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica establece el marco regulador de la política de seguridad de la información, el cual debe plasmarse en un documento accesible y comprensible para todos los miembros de la organización. Dicho documento definirá lo que significa seguridad de la información y establecerá la forma en que la organización gestiona y protege la información y los servicios que considera críticos. Además, la política de seguridad de la información debe ser coherente con lo establecido en el Documento de Seguridad que exige el artículo 88 del Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, aprobado por Real Decreto 1720/2007, de 21 de diciembre.

La Consejería de Justicia e Interior es consciente de la necesidad y la importancia de avanzar en esta regulación para proteger los activos de información que se gestionan en el ámbito de la administración electrónica, dado el creciente peso de los tratamientos plenamente automatizados y el carácter sensible de los datos manejados en su ámbito de gestión.

De una parte, el artículo 10 del Decreto 1/2011, de 11 de enero, por el que se establece la política de seguridad de las tecnologías de la información y comunicaciones en la Administración de la Junta de Andalucía, dispone que en cada entidad incluida en su ámbito de aplicación se creará un Comité de Seguridad TIC, como órgano colegiado de dirección y seguimiento en materia de seguridad de los activos TIC de su titularidad o cuya gestión tenga encomendada. La composición, atribuciones, funcionamiento y método de trabajo del Comité de Seguridad TIC deberá ser aprobada por el máximo órgano de dirección de la entidad, en el caso de las Consejerías mediante Orden de la persona titular.

De otra parte, el artículo 11.1 del Real Decreto 3/2010, de 8 de enero, establece que todos los órganos superiores de las Administraciones públicas deberán disponer formalmente de su política de seguridad, que será aprobada por el titular del órgano superior correspondiente, entendiendo a estos efectos, en su apartado 2, como órganos superiores a los responsables directos de la ejecución del gobierno autonómico de acuerdo con lo previsto en los estatutos de autonomía correspondiente y normas de desarrollo. De este modo, según se dispone en el artículo 16 de la Ley 9/2007, de 22 de octubre, de la Administración de la Junta de Andalucía, la Consejería de Justicia e Interior es un órgano superior que integra la estructura básica de la Administración de la Junta de Andalucía, bajo la superior dirección del Consejo de Gobierno.

De acuerdo con lo anterior, mediante esta Orden se establece la política de seguridad de la información en el ámbito de la Administración electrónica de la Consejería de Justicia e Interior, así como el marco organizativo y tecnológico.

En su virtud, de acuerdo con lo dispuesto en el artículo 44.2 de la Ley 6/2006, de 24 de octubre, del Gobierno de la Comunidad Autónoma de Andalucía, en el artículo 26.2.a) de la Ley 9/2007, de 22 de octubre,

de la Administración de la Junta de Andalucía, y en el Decreto 148/2012, de 5 de junio, por el que se establece la estructura orgánica de la Consejería de Justicia e Interior,

D I S P O N G O

Artículo 1. Objeto.

El objeto de esta Orden es establecer la política de seguridad de la información en el ámbito de la Administración Electrónica de la Consejería de Justicia e Interior, así como el marco organizativo y tecnológico.

Artículo 2. Objetivos de la política de seguridad de la información.

Son objetivos de la política de seguridad de la información:

a) Garantizar la seguridad de la información, proteger los activos o recursos de información.

b) Crear la estructura de seguridad de la Consejería de Justicia e Interior.

c) Marcar las directrices, los objetivos y los principios básicos de seguridad de la información de la organización.

d) Orientar la organización para la prestación de servicios basados en la gestión de riesgos.

e) Servir de base para el desarrollo de las normas, procedimientos y procesos de gestión de la seguridad de la información.

Artículo 3. Ámbito de aplicación.

La política de seguridad de la información se aplicará a todos los sistemas de información gestionados por la Consejería de Justicia e Interior, siempre que sean utilizados en el ámbito de la Administración General, por alguno de los órganos o unidades administrativas, centrales o periféricos, de la Consejería de Justicia e Interior. Asimismo, deberá ser observada por todo el personal de la Administración General destinado en dichos órganos y unidades administrativas, así como por aquellas personas que, aunque no destinadas en ellos, tengan acceso a sus sistemas de información.

Artículo 4. Principios básicos.

Los principios básicos que regirán la política de seguridad de la información de la Consejería de Justicia e Interior, además de los establecidos en el Decreto 1/2011, de 11 de enero, por el que se establece la política de seguridad de las tecnologías de la información y comunicaciones en la Administración de la Junta de Andalucía, son los siguientes:

a) Principio de prevención. Se evitará, o al menos prevendrá en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad. Para ello, se deben implementar las medidas mínimas de seguridad determinadas por las normas y leyes que le sean de aplicación, así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos. Estos controles, y los roles y responsabilidades de seguridad de todo el personal, estarán claramente definidos y documentados.

b) Principio de detección. Dado que los servicios se pueden degradar rápidamente debido a incidentes que, en función de su gravedad, pueden producir desde una simple desaceleración hasta la detención de los mismos, se debe monitorizar la operación de los servicios de manera continua para detectar anomalías en los niveles de prestación requeridos, actuando en consecuencia. La monitorización es especialmente relevante para establecer líneas de defensa. Para ello, se implantarán mecanismos de detección, análisis y reporte que lleguen a las personas responsables regularmente, a efectos de detectar cuándo se produce una desviación significativa de los parámetros de servicio marcados.

c) Principio de reacción. Deberá minimizarse el tiempo requerido de recuperación, de forma que el impacto de los incidentes de seguridad sea el menor posible, para lo cual se establecerán mecanismos para responder eficazmente a los incidentes de seguridad, designando un punto de contacto para centralizar y gestionar el intercambio de información asociada a los incidentes de seguridad, así como estableciendo protocolos para el intercambio de información relacionada con dichos incidentes.

d) Principio de recuperación. Se deberá garantizar en la medida de lo posible la disponibilidad de los servicios ofrecidos a la ciudadanía, en función de la criticidad de los mismos.

e) Principio de responsabilidad. Todas las personas que de una forma u otra participen en la utilización, operación, administración o gestión de un sistema de información, serán responsables de observar las normas de seguridad establecidas. Para ello las correspondientes responsabilidades deberán quedar determinadas de forma explícita, y ser comunicadas a cada una de ellas.

00061726

Artículo 5. Estructura organizativa de la política de seguridad de la información.

La estructura organizativa de gestión de la seguridad de la información en el ámbito de la Consejería de Justicia e Interior estará compuesta por los siguientes agentes:

a) Comité de Seguridad de las Tecnologías de la Información y las Comunicaciones.
b) Responsable de la Seguridad.
c) Responsables de la Información.
d) Responsables de los Servicios.
e) Responsables de los Sistemas.

Artículo 6. El Comité de Seguridad de las Tecnologías de la Información y Comunicaciones.

1. Se crea el Comité de Seguridad de las Tecnologías de la Información y las Comunicaciones de la Consejería de Justicia e Interior, en adelante Comité de Seguridad TIC, como órgano colegiado de dirección y seguimiento en materia de seguridad TIC, de conformidad con lo previsto en el artículo 10 del Decreto 1/2011, de 11 de enero.

2. Corresponde al Comité de Seguridad TIC el ejercicio de las siguientes funciones:

a) Aprobar el desarrollo de la política de seguridad de la información de segundo nivel.

b) Velar por el desarrollo, implantación, concienciación, formación y divulgación, así como por el cumplimiento y actualización de la política de seguridad de la información en la Consejería de Justicia e Interior.

c) Planificar y priorizar las iniciativas necesarias para cumplir con las directrices, los objetivos y los principios básicos marcados en la presente Política de seguridad de la información. En especial, la elaboración, actualización y reevaluación periódica de los análisis de riesgos necesarios.

d) Proporcionar, dentro de los límites establecidos en los programas asignados por las leyes anuales de presupuestos a la Consejería de Justicia e Interior, los medios y recursos necesarios para posibilitar la realización de las iniciativas planificadas.

e) Coordinar a alto nivel todas las actuaciones de seguridad, velando para que la definición y el desarrollo de las mismas se adecuen en todo momento a las directrices marcadas por la política de seguridad de la información, involucrando a las diferentes áreas implicadas.

f) Velar para que todos los ámbitos de responsabilidad y actuación en relación a la seguridad de la información y su tratamiento queden perfectamente definidos, aprobando los nombramientos necesarios para ello. Especialmente, para asegurar que todos y cada uno de los miembros de la estructura de seguridad definida conozcan sus funciones y responsabilidades.

g) Promover y fomentar la divulgación y formación en cultura de la seguridad de la información, así como la mejora continua de la seguridad en la organización y en todas sus entidades dependientes, aprobando los planes de mejora de seguridad de la información propuestos por el Responsable de la Seguridad, y velando por la asignación y cumplimiento de las responsabilidades oportunas.

h) 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.

i) Asegurar que el desarrollo normativo que tenga incidencia en el desarrollo o explotación de sistemas de información se adecua a lo establecido en la política de seguridad de la información.

j) Resolver los conflictos que puedan aparecer entre las diferentes personas responsables o entre diferentes áreas de la organización en materia de seguridad de la información.

k) Aprobar el documento de seguridad en los términos exigidos por la normativa de protección de datos de carácter personal.

3. El Comité de Seguridad TIC estará integrado por los siguientes miembros:

a) Presidencia: la persona titular de la Viceconsejería.
b) Vicepresidencia: la persona titular de la Secretaría General Técnica.
c) Vocalías: las personas titulares de todos los órganos directivos centrales.
d) Secretaría: la persona titular de la jefatura del Servicio de Informática, con voz y voto. En los casos de vacante, ausencia, enfermedad u otra causa legal, será sustituida por una persona adscrita al Servicio de Informática, con la misma cualificación y requisitos que su titular, nombrada por la presidencia del Comité de Seguridad TIC.

4. El Responsable de la Seguridad asistirá en calidad de asesor a las reuniones del Comité de Seguridad TIC, salvo que puntualmente se disponga lo contrario de forma expresa por parte de la presidencia. El Comité de Seguridad TIC podrá convocar a sus reuniones a las personas que en cada caso autorice la presidencia, a propuesta de alguno de sus miembros. Asimismo podrá recabar de personal técnico especializado, propio o externo, la información pertinente para la toma de decisiones.

5. El Comité de Seguridad TIC se reunirá con carácter ordinario una vez al año y con carácter extraordinario por acuerdo de la presidencia, a iniciativa propia o previa solicitud razonada de uno de sus miembros.

6. El Comité de Seguridad TIC se regirá por la presente Orden, por las normas sobre los órganos colegiados de la sección 1.ª del Capítulo II del Título IV de la Ley 9/2007, de 22 de octubre, de la Administración de la Junta de Andalucía, y, en lo que sea de aplicación, por 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.

Artículo 7. Responsable de la Seguridad.

1. El Responsable de la Seguridad será una persona adscrita al Servicio de Informática nombrado por el Comité de Seguridad TIC, a propuesta de la persona titular de la jefatura del Servicio de Informática.

2. Serán funciones del Responsable de la Seguridad, dentro de su ámbito de actuación, las siguientes:

a) Proponer temas a tratar en las reuniones del Comité de Seguridad TIC, asesorando y aportando información para la toma de decisiones.

b) Analizar y proponer al Comité de Seguridad TIC cualquier medida que considere necesaria para satisfacer los requisitos de seguridad de la información y de los servicios prestados.

c) Velar por la correcta ejecución de los procedimientos y procesos operativos de seguridad, coordinando las medidas a adoptar por los diferentes actores involucrados en la gestión de la seguridad de la información, analizando asimismo la adecuación de los mismos a la normativa establecida.

d) Definir y coordinar las medidas operativas, en función de las directrices marcadas por el Comité de Seguridad TIC, realizando el seguimiento de las actuaciones relacionadas con la seguridad TIC de los activos de información de la Consejería y con la gestión del riesgo.

e) Coordinar los programas de formación y concienciación, apoyando al Comité de Seguridad TIC en la definición de las acciones formativas necesarias para satisfacer los requisitos marcados por este.

f) Asesorar, en colaboración con los Responsables de los Sistemas, a los Responsables de la Información y a los Responsables de los Servicios en el proceso de la gestión de los riesgos, así como elevar un informe anual sobre el estado del proceso al Comité de Seguridad TIC.

g) Promover y realizar el seguimiento de las auditorías periódicas que den cumplimiento a las obligaciones en materia de seguridad de la información y de los datos de carácter personal, de acuerdo al calendario aprobado por el Comité de Seguridad TIC.

h) Analizar los informes de auditoría, elaborando las conclusiones que presentará al Comité de Seguridad TIC, transmitiendo con posterioridad los resultados a las diferentes personas responsables para que adopten las medidas correctoras oportunas.

i) Elaborar informes periódicos de seguridad para el Comité de Seguridad TIC, con inclusión y estudio de los incidentes más relevantes de cada período y la gestión realizada de los mismos, así como de los principales riesgos residuales asumidos por la organización, recomendando posibles actuaciones respecto de ellos.

j) Velar para que la documentación de difusión limitada sea custodiada de forma adecuada.

Artículo 8. Responsables de la Información.

1. Los Responsables de la Información serán las personas titulares de los centros directivos que decidan sobre la finalidad, contenido y uso de la información.

2. Las principales funciones, dentro de su ámbito de actuación, son las siguientes:

a) Ayudar a determinar los requisitos de seguridad de la información, categorizando la información mediante la valoración de los impactos de los incidentes que puedan producirse.

b) Proporcionar la información necesaria al Responsable de la Seguridad para realizar los preceptivos análisis de riesgos, con la finalidad de establecer las salvaguardas a implantar. Para ello contará con la ayuda de los Responsables de los Servicios y de los Responsables de los Sistemas.

c) Verificar que los análisis de riesgos realizados se corresponden en todo momento con la información aportada para la realización de los mismos.

00061726

Artículo 9. Responsables de los Servicios.

1. Los Responsables de los Servicios serán las personas titulares de los centros directivos que decidan sobre las características de los servicios a prestar.

2. Las principales funciones, dentro de su ámbito de actuación, son las siguientes:

a) Ayudar a determinar los requisitos de seguridad de los servicios a prestar, categorizando los servicios mediante la valoración de los impactos de los incidentes que puedan producirse.

b) Proporcionar la información necesaria al Responsable de la Seguridad para realizar los preceptivos análisis de riesgos, con la finalidad de establecer las salvaguardas a implantar. Para ello contará con la ayuda de los Responsables de la Información y de los Responsables de los Sistemas.

c) Verificar que los análisis de riesgos realizados se corresponden en todo momento con la información aportada para la realización de los mismos.

Artículo 10. Responsables de los Sistemas.

1. Los Responsables de los Sistemas serán personas adscritas al Servicio de Informática designadas al efecto por la persona titular de la jefatura y figurarán en la documentación de seguridad de los sistemas de información. Para cada sistema de información deberá existir un Responsable de Sistema, siendo posible que una misma persona sea responsable de varios sistemas.

2. Sus principales responsabilidades serán:

a) Supervisar el desarrollo, operación y mantenimiento de los sistemas de información durante todo su ciclo de vida, así como las especificaciones de los mismos, la instalación y verificación de su correcto funcionamiento.

b) Ser el primer responsable de la seguridad de los sistemas de información que dirija, velando porque la seguridad de la información esté presente en todas y cada una de las partes de sus ciclos de vida. Especialmente deberá velar porque el desarrollo de los sistemas siga las directrices de seguridad establecidas de manera horizontal por la Junta de Andalucía. Para todo ello podrá contar con el asesoramiento del Responsable de la Seguridad.

c) Creación, mantenimiento y actualización continua de la documentación de seguridad de los sistemas de información, con el asesoramiento del Responsable de la Seguridad.

d) Asesorar en la definición de la topología y sistema de gestión de los sistemas de información estableciendo los criterios de uso y los servicios disponibles en el mismo.

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

f) Cerciorarse de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad.

g) Asesorar en colaboración con el Responsable de la Seguridad, a los Responsables de la Información y a los Responsables de los Servicios, en el proceso de la gestión de riesgos.

h) Suspender el manejo de una cierta información o la prestación de un cierto servicio si es informado de deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos. Esta decisión debe ser acordada con los responsables de la información afectada, del servicio afectado y con el Responsable de la Seguridad, antes de ser ejecutada.

Artículo 11. Resolución de conflictos.

1. Los conflictos entre las diferentes personas responsables que componen la estructura organizativa de la política de seguridad de la información serán resueltos por el superior jerárquico. En su defecto, prevalecerá la decisión del Comité de Seguridad TIC.

2. En los conflictos entre las personas responsables que componen la estructura organizativa de la política de seguridad de la información y las personas responsables definidas en la normativa de protección de datos de carácter personal prevalecerá la decisión que presente un mayor nivel de exigencia respecto a la protección de los datos de carácter personal.

Artículo 12. Obligaciones del personal.

1. Todo el personal que preste servicios en la Consejería de Justicia e Interior tiene la obligación de conocer y cumplir la política de seguridad de la información y la normativa de seguridad derivada, siendo responsabilidad del Comité de Seguridad TIC disponer los medios necesarios para que la información llegue a las personas afectadas.

2. Todo el personal que se incorpore a la Consejería de Justicia e Interior o vaya a tener acceso a alguno de sus sistemas de información o la información gestionada por ellos deberá ser informado de la política de seguridad de la información.

3. Procederá el ejercicio de las acciones pertinentes para la exigencia de las responsabilidades legales que correspondan por el incumplimiento manifiesto de la política de seguridad de la información o de la normativa de seguridad derivada.

4. El personal empleado público al servicio de la Junta de Andalucía deberán cumplir además la Resolución de 27 de septiembre de 2004, de la Secretaría General para la Administración Pública, por la que se establece el manual de comportamiento de los empleados públicos en el uso de los sistemas informáticos y redes de comunicaciones de la Administración de la Junta de Andalucía.

Artículo 13. Desarrollo.

1. Las medidas sobre la seguridad de la información, de obligado cumplimiento, se desarrollarán en cuatro niveles con diferente ámbito de aplicación, detalle técnico y obligatoriedad de cumplimiento, pero de manera que cada elemento de desarrollo se fundamente en el nivel superior. Dichas medidas conformarán el Plan Director de Seguridad de los Sistemas de Información de la Consejería de Justicia e Interior.

Todos estos niveles prestarán especial atención a las exigencias derivadas del Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, así como a la normativa aplicable en materia de protección de datos de carácter personal.

Los niveles de desarrollo son los siguientes:

a) Primer nivel: política de seguridad de la información, constituido por la presente orden. Es de obligado cumplimiento en toda la Consejería de Justicia e Interior.

b) Segundo nivel: normas de seguridad. Son de obligado cumplimiento en toda la Consejería de Justicia e Interior y deben ser aprobadas por el Comité de Seguridad TIC. Describen de forma general los principios y normas de seguridad que serán concretados en los niveles posteriores.

c) Tercer nivel: procedimientos. Describen las acciones a realizar, de una manera más específica, en un proceso relacionado con la seguridad. Son dependientes de las normas de seguridad.

d) Cuarto nivel: Documentación técnica. En este último nivel se puede incluir todo tipo de documentación técnica o especializada que se considere necesario para completar y facilitar el desarrollo de las medidas de seguridad.

2. El Comité de Seguridad TIC establecerá los mecanismos necesarios para compartir la documentación derivada del desarrollo con el propósito de regularizarlo, en la medida de lo posible, en todo el ámbito de aplicación de la política de seguridad de la información.

La siguiente tabla resume el marco de desarrollo y la responsabilidad de su aprobación:

Nivel	Documento	Aprueba
Primero	Política de seguridad	Persona titular de la Consejería de Justicia e Interior
Segundo	Normas de seguridad	Comité de Seguridad TIC
Tercero	Procedimientos	Persona titular de la Secretaría General Técnica
Cuarto	Documentación técnica	Persona titular d e la jefatura del Servicio de Informática

Artículo 14. Gestión de riesgos.

1. La gestión de riesgos deberá realizarse de manera continua sobre el sistema de información, conforme a los principios de gestión de la seguridad basada en los riesgos y con reevaluación periódica de los mismos.

2. Las personas encargadas de la categorización de los sistemas serán los Responsables de la Información y de los Servicios, siendo el Responsable de la Seguridad la persona encargada de supervisar los análisis de riesgos y proponer las medidas de seguridad a aplicar.

3. Los Responsables de la Información y de los Servicios son las personas responsables de aceptar los riesgos residuales calculados en el análisis sobre la información y los servicios, respectivamente, y de realizar 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 al menos con periodicidad anual por parte del Responsable de la Seguridad, que elevará un informe al Comité de Seguridad TIC.

Artículo 15. Protección de datos de carácter personal.

1. Los ficheros con datos de carácter personal estarán reflejados en el correspondiente Documento de Seguridad, donde se hará constar tanto los ficheros afectados como las personas responsables correspondientes.

00061726

2. Todos los sistemas de información de la Consejería de Justicia e Interior 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 prevalecerá la norma que presente un mayor nivel de exigencia respecto a la protección de los datos de carácter personal.

Disposición adicional primera. Constitución del Comité de Seguridad TIC.

La primera reunión del Comité de Seguridad TIC tendrá por objeto la constitución del mismo y se celebrará en un plazo máximo de treinta días a partir de la entrada en vigor de la presente orden. En dicha reunión se procederá al nombramiento del Responsable de la Seguridad y de los Responsables de la Información y de los Servicios. Anteriormente deberán estar ya nombrados los Responsables de los Sistemas.

Disposición adicional segunda. Deber de colaboración de órganos y unidades de la Consejería.

Todos los órganos y unidades de la Consejería prestarán su colaboración en las actuaciones de implementación de la política de seguridad de la información aprobada por esta Orden.

Disposición adicional tercera. Actualización permanente y revisiones periódicas.

1. Esta Orden deberá mantenerse actualizada para adecuarla al progreso de los servicios de la Administración electrónica, a la evolución tecnológica y al desarrollo de la sociedad de la información, así como a los estándares internacionales de seguridad.

2. Las propuestas de las sucesivas revisiones de la política de seguridad de la información las hará el Comité de Seguridad TIC.

Disposición final primera. Publicidad de la política de seguridad de la información.

La presente Orden se publicará, además de en el Boletín Oficial de la Junta de Andalucía, en los medios que se establezcan por el Comité de Seguridad TIC.

Disposición final segunda. Entrada en vigor.

La presente Orden entrará en vigor el día de su publicación en el Boletín Oficial de la Junta de Andalucía.

Sevilla, 22 de diciembre de 2014

EMILIO DE LLERA SUÁREZ-BÁRCENA
Consejero de Justicia e Interior

00061726