3. Otras disposiciones

CONSEJERÍA DE EMPLEO, EMPRESA Y COMERCIO

ORDEN de 9 de junio de 2016, por la que se efectúa el desarrollo de la política de seguridad de las tecnologías de la información y comunicaciones en la Administración de la Junta de Andalucía.

El uso de las tecnologías de la información y comunicaciones es vital, como en la mayoría de las organizaciones actuales, para el desarrollo eficiente de buena parte de las actividades cotidianas de los organismos y entidades de la Junta de Andalucía. La información, así como los procesos y sistemas que hacen uso de ella, constituyen elementos esenciales para su buen funcionamiento.

Esta Administración es consciente de la importancia que ha de concederse a que los activos sean gestionados conforme a estándares, buenas prácticas de seguridad y con pleno cumplimiento de la legislación aplicable en la materia, como elemento clave de la confianza de la ciudadanía en los servicios públicos digitales y de la adecuada gestión de sus datos.

En este sentido, la Junta de Andalucía ha venido manteniendo en el tiempo un compromiso continuo con la seguridad de los sistemas de información. Buena muestra de ello fue la aprobación, mediante Acuerdo de Consejo de Gobierno de fecha 16 de noviembre de 2010, del Plan Director de Seguridad de los Sistemas de Información y Telecomunicaciones de la Administración de la Junta de Andalucía (2010-2013), así como del Decreto 1/2011, de 11 de enero, por el que se estableció la política de seguridad de las tecnologías de la información y comunicaciones en la Administración de la Junta de Andalucía.

Dicho Decreto 1/2011, de 11 de enero, a la vez que se configura como una norma vertebradora, deja sentados los objetivos y criterios básicos para el tratamiento de la seguridad de los sistemas de información y determina los pilares del marco regulador, así como la estructura organizativa y de gestión encargada de velar por su cumplimiento en la Junta de Andalucía previendo, en su disposición final primera, la facultad del Consejero competente en materia de innnovación para dictar cuantas disposiciones sean precisas para el desarrollo y ejecución de lo previsto en el citado Decreto.

Además, mediante el mismo también se da respuesta a varios mandatos legales y reglamentarios en materia de seguridad de la información, entre ellos, a la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, la cual, en su artículo 9.1, obliga a las personas responsables de los ficheros que contengan datos personales a «adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado», así como a lo establecido en el Real Decreto 3/2010, de 8 de enero, por el que se aprueba el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, que obliga a los órganos superiores de las Administraciones Públicas a dotarse formalmente de una política de seguridad, que deberá atenerse a los principios básicos y requisitos mínimos definidos en dicho real decreto.

Precisamente, esta última norma propugna que la política de seguridad se desarrolle a través de un conjunto de documentos cuyo objetivo sea facilitar que el tratamiento de información se realice de acuerdo con los objetivos y principios expuestos en la misma.

Por otro lado, la disposición final octava de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos establece que corresponde al Gobierno y a las Comunidades Autónomas, en el ámbito de sus respectivas competencias, dictar las disposiciones necesarias para el desarrollo y aplicación de la citada Ley.

Por consiguiente, se configura como objeto central de la presente disposición la habilitación de un instrumento normativo ágil, habida cuenta del vertiginoso ritmo con que evoluciona el sector de las nuevas tecnologías y la imperiosa necesidad de adaptarse a él de forma permanente y rápida, para regular diferentes aspectos o ámbitos de la seguridad de la información en el marco de la Junta de Andalucía, convirtiéndose así en un elemento clave para el desarrollo de la política de seguridad de las tecnologías de la información y comunicaciones en la Administración de la Junta de Andalucía y, paralelamente, en las entidades que formarán parte del alcance de esta Orden.

Esta disposición también pretende convertirse, así, en un instrumento facilitador y, por ende, impulsor, del cumplimiento normativo por parte de los organismos y entidades de la Junta de Andalucía, en el ámbito de la seguridad de la información y más específicamente del Esquema Nacional de Seguridad, ofreciendo un marco general de actuación a sus diferentes entidades integrantes que permitirá alinear y homogeneizar sus esfuerzos de adecuación al nuevo marco normativo europeo y estatal, y también aligerar, en parte, dichos esfuerzos, al poder aquéllas asumir como propias las resoluciones y la documentación técnica que se deriven del desarrollo

00093220

de esta Orden, sin perjuicio de las propias disposiciones que ellas mismas elaboren para la plena satisfacción de sus requisitos específicos.

Esta regulación se efectuará mediante futuras resoluciones (integradas por normas de seguridad) y documentos técnicos de actualización periódica (integradas por procedimientos de seguridad y guías técnicas).

Para la elaboración de esta Orden también se ha tenido en cuenta lo establecido en 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, publicado mediante Resolución de 27 de septiembre de 2004, de la Secretaría General para la Administración Pública. En este sentido, el desarrollo que se derive de la presente Orden se realizará, en aquellos ámbitos en los que exista una coincidencia o afinidad temática entre ambas disposiciones, en coherencia y complementariedad con lo dispuesto en la mencionada Resolución.

En la medida en que se considera necesario que determinados extremos de estos documentos sean establecidos por parte del órgano competente con carácter de obligado cumplimiento y conocidos por todos los agentes afectados de su ámbito de aplicación, se ha decidido formalizar su adopción a través de la presente Orden, la cual se ha estructurado en tres capítulos, bajo las rúbricas «Disposiciones generales», «Ámbitos en materia de seguridad de la información que serán objeto de desarrollo mediante resoluciones y documentos técnicos», así como «Difusión del marco normativo», a los que se añaden tres disposiciones finales por las que se establecen la potestad para el desarrollo de esta Orden, la disponibilidad de créditos y plazos y la fecha de su entrada en vigor, respectivamente.

En virtud de lo expuesto, de acuerdo con lo dispuesto en el artículo 26.2.a) de la Ley 9/2007, de 22 de octubre, de la Administración de la Junta de Andalucía, el artículo 44.2 de la Ley 6/2006, de 24 de octubre, del Gobierno de la Comunidad Autónoma de Andalucía, el Decreto de la Presidenta 12/2015, de 17 de junio, de la Vicepresidencia y sobre reestructuración de Consejerías, el Decreto 210/2015, de 14 de julio, por el que se regula la estructura orgánica de la Consejería de Empleo, Empresa y Comercio y la disposición final primera del Decreto 1/2011, de 11 de enero,

D I S P O N G O

CAPÍTULO I

Disposiciones generales

Artículo 1. Objeto y ámbito de aplicación.

1. El objeto de la presente Orden es establecer las bases para el desarrollo de la política de seguridad de las tecnologías de la información y comunicaciones en los organismos y entidades de la Junta de Andalucía, facilitando así que el tratamiento de la información se realice de acuerdo con los objetivos y principios expuestos en la misma.

2. Esta disposición será de aplicación a la Administración de la Junta de Andalucía y a sus entidades instrumentales, así como a los consorcios a los que se refiere el artículo 12.3 de la Ley 9/2007, de 22 de octubre, de la Administración de la Junta de Andalucía.

Artículo 2. Documentación de desarrollo.

1. La política de seguridad de las tecnologías de la información y comunicaciones en los organismos y entidades de la Junta de Andalucía se desarrollará a través de resoluciones de la Dirección General competente en materia de coordinación y ejecución de las políticas de seguridad de los sistemas de información y telecomunicaciones de la Administración de la Junta de Andalucía, así como mediante documentos técnicos, que se agruparán en las categorías de procedimientos y guías técnicas.

2. Las resoluciones y documentos técnicos se aprobarán de acuerdo con los centros directivos que correspondan cuando, en su caso, las materias específicas reguladas puedan tener relación con elementos de su competencia.

3. Las resoluciones proporcionarán un primer nivel de concreción y cada una de ellas estará asociada a uno o varios de los ámbitos en materia de seguridad de la información definidos en el capítulo II. Los procedimientos describirán la secuencia concreta de actividades que permiten satisfacer las obligaciones contenidas en las normas. Las guías técnicas ofrecerán información sobre cómo actuar ante situaciones y tecnologías específicas.

4. Los procedimientos y guías técnicas tendrán carácter de recomendaciones y serán desarrollados, por cada organismo o entidad, con arreglo a los ámbitos en materia de seguridad de la información que se establezcan.

5. Cada entidad podrá ampliar y desarrollar, sobre la base de los mínimos establecidos, las resoluciones que se aprueben.

6. Se utilizará un lenguaje no sexista en la elaboración y redacción de las resoluciones y documentos técnicos que se deriven de esta Orden, así como en aquellos otros que desarrollen la política de seguridad de la información en cada una de las entidades y organismos incluidos en el ámbito de aplicación de la presente Orden.

CAPÍTULO II

Ámbitos en materia de seguridad de la información que serán objeto de desarrollo mediante resoluciones y documentos técnicos

Artículo 3. Acceso y uso de aplicaciones corporativas, servicios de Internet y otros recursos de uso colectivo o individual.

Será objeto de tratamiento dentro de este ámbito, habida cuenta de que la utilización de equipamiento informático y de comunicaciones es actualmente una necesidad en cualquier organización del sector público, la definición de los criterios de uso seguro de los medios y recursos TIC que se ponen a disposición del personal que presta sus servicios en cada entidad incluida en el ámbito de aplicación de esta Orden.

Especialmente, los aspectos desarrollados en este ámbito serán complementarios y coherentes con los establecidos en 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, publicado mediante Resolución de 27 de septiembre de 2004, de la Secretaría General para la Administración Pública.

Artículo 4. Tratamiento seguro de la información y sus soportes.

Será objeto de desarrollo dentro de este ámbito el conjunto de aspectos relacionados con el almacenamiento, acceso, transmisión, distribución y destrucción de la información manejada por cada entidad incluida en el ámbito de aplicación de esta Orden, así como de sus soportes, ya sean medios electrónicos o cualquier otro en que se materialice la información.

También será objeto de desarrollo en este ámbito la clasificación de la información y, ligados a ella, el marcado y tratamiento que se debe dar a la misma. Esta clasificación permite establecer diferencias entre las medidas de seguridad a aplicar a cada tipo de información, según su importancia relativa y atendiendo a criterios de disponibilidad, integridad y confidencialidad de los datos.

Artículo 5. Seguridad ligada al personal.

Será objeto de tratamiento dentro de este ámbito garantizar que el personal que presta sus servicios en los organismos y entidades incluidas en el ámbito de aplicación de esta Orden es consciente de sus obligaciones y responsabilidades en materia de seguridad y que, en todo caso, recibe la formación y capacitación adecuada.

Artículo 6. Gestión de incidentes de seguridad, registro de eventos y continuidad del servicio.

Será objeto de tratamiento dentro de este ámbito la definición de los mecanismos para que los eventos relacionados con la seguridad sean detectados en una fase temprana, notificados a los agentes responsables que correspondan y tratados de una forma adecuada.

Asimismo, será objeto de desarrollo dentro de este ámbito la definición de los mecanismos para que cada entidad tenga la capacidad de registrar la actividad desarrollada sobre el sistema, de forma que pueda saberse a posteriori quién realiza cada actividad, cuándo la realiza y sobre qué información, con el propósito de identificar anomalías, responsables y elementos de mejora que incidan en un aumento de la seguridad de dicho sistema.

Finalmente, también se tratará de establecer mecanismos para contrarrestar el impacto sobre los procesos críticos de la organización derivado de catástrofes o fallos importantes relacionados con los sistemas de información y garantizar la reanudación de la actividad.

Artículo 7. Contratación y relaciones con terceros.

Será objeto de desarrollo dentro de este ámbito el mantenimiento de la seguridad de los datos, las aplicaciones y los sistemas de la organización que sean objeto de tratamiento, desarrollo, suministro o administración por parte de terceros, en el marco de una contratación o cualquier otro tipo de vinculación o acuerdo entre partes.

Artículo 8. Protección lógica de equipos, electrónica de red, comunicaciones y servicios.

Será objeto de desarrollo dentro de este ámbito la definición de mecanismos para disponer de una configuración segura en los distintos dispositivos de procesamiento o de interconexión de red del sistema, de forma que se minimice su vulnerabilidad frente a posibles ataques o errores de uso, así como la disposición de herramientas y recursos que permitan prevenir ataques o, en su caso, detectarlos y reaccionar antes ellos.

00093220

Artículo 9. Seguridad de las aplicaciones software.

Será objeto de desarrollo dentro de este ámbito la definición de los criterios para lograr un adecuado nivel de seguridad en el software utilizado en cada organismo o entidad que forme parte del ámbito de aplicación de esta Orden, considerando para ello todo su ciclo de vida, desde la planificación de su desarrollo hasta su retirada del servicio, pasando por su desarrollo o adquisición y su posterior mantenimiento.

Artículo 10. Protección física de equipos y acondicionamiento y protección de instalaciones.

Será objeto de desarrollo dentro de este ámbito la operativa que se ha de implementar en cada organismo o entidad que forme parte del ámbito de aplicación de esta Orden para evitar accesos físicos no autorizados a las instalaciones con equipamiento TIC y para prevenir circunstancias accidentales que puedan afectar a la actividad normal de la organización.

De forma particular, los aspectos desarrollados en este ámbito serán complementarios y coherentes con los establecidos en el Decreto 94/2014, de 27 de mayo, por el que se aprueba la norma técnica para la protección de edificios públicos de uso administrativo ante el riesgo de intrusión.

Artículo 11. Caracterización y planificación de los sistemas.

Será objeto de desarrollo dentro de este ámbito la operativa que se ha de implementar en cada organismo o entidad que forme parte del ámbito de aplicación de esta Orden para lograr una caracterización de los sistemas tanto en el momento actual como a lo largo del tiempo, de manera que, a partir de un conocimiento detallado de los sistemas, sea posible establecer en cada momento un conjunto adecuado de medidas de seguridad y, asimismo, planificar de un modo ordenado y controlado la evolución de dichos sistemas para que siempre cumplan su función bajo unos parámetros de seguridad adecuados.

Artículo 12. Auditoría.

Serán objeto de desarrollo dentro de este ámbito los procesos que tratan de sustentar, mediante auditorías, la confianza que merecen los sistemas en materia de seguridad. Es decir, de calibrar su capacidad para garantizar la integridad, disponibilidad, autenticidad, confidencialidad y trazabilidad de los servicios prestados y la información tratada, almacenada o transmitida.

Precisamente, a través de la auditoría, se pretende obtener una opinión independiente y objetiva sobre este cumplimiento, de tal forma que permita a los responsables correspondientes, tomar las medidas oportunas para, en su caso, subsanar las deficiencias identificadas y para infundir internamente o bien a terceros la confianza sobre el nivel de seguridad alcanzado.

CAPÍTULO III

Difusión del marco normativo

Artículo 13. Divulgación y formación.

A los efectos de dar a conocer y facilitar el cumplimiento del marco normativo, la Consejería competente en materia de coordinación y ejecución de las políticas de seguridad de los sistemas de información y telecomunicaciones de la Administración de la Junta de Andalucía, habilitará los medios necesarios para hacer accesibles las distintas resoluciones y documentos técnicos, impulsando, asimismo, la puesta en marcha de los programas formativos y divulgativos necesarios.

Disposición final primera. Disponibilidad de créditos y plazos.

Las actuaciones que se deriven de la aplicación efectiva de esta Orden deberán ser atendidas con los presupuestos disponibles para esta materia en cada organismo o entidad, con previsión de los correspondientes mecanismos de control y fiscalización del gasto, de manera que las iniciativas a llevar a cabo estarán siempre limitadas, en lo que respecta a los plazos de ejecución, por las disponibilidades presupuestarias existentes.

Disposición final segunda. Entrada en vigor.

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

Sevilla, 9 de junio de 2016

JOSÉ SÁNCHEZ MALDONADO
Consejero de Empleo, Empresa y Comercio

00093220