3. Otras disposiciones

CONSEJERÍA DE EMPLEO, EMPRESA Y COMERCIO

Resolución de 13 de julio de 2018, de la Dirección General de Telecomunicaciones y Sociedad de la Información, por la que se establecen normas sobre gestión de incidentes de seguridad TIC.

Se constatan los siguientes,

ANTECEDENTES DE HECHO

Primero. En virtud del Decreto 210/2015, de 14 de julio, por el que se regula la estructura orgánica de la Consejería de Empleo, Empresa y Comercio, y de acuerdo con el Decreto de la Presidenta 12/2015, de 17 de junio, de la Vicepresidencia y sobre reestructuración de Consejerías, a la Consejería de Empleo, Empresa y Comercio le corresponden las competencias atribuidas a la Comunidad Autónoma de Andalucía relativas a la dirección e impulso de la política de telecomunicaciones y seguridad de los sistemas de información de la Administración de la Junta de Andalucía y del sector público andaluz. En concreto, según el artículo 12.2. i) del Decreto 210/2015, de 14 de julio, le corresponde la «Coordinación y ejecución de las políticas de seguridad de los sistemas de Información y telecomunicaciones de la Administración de la Junta de Andalucía».

Segundo. 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, establece entre los principios básicos en materia de seguridad de la información los de prevención, reacción y recuperación, y fija directrices generales para la adecuada gestión de los incidentes de seguridad.

Tercero. La Resolución de 13 de abril de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Notificación de Incidentes de Seguridad establece los criterios de determinación del nivel de Impacto de los incidentes y la notificación obligatoria al Centro Criptológico Nacional (CCN) de los incidentes con nivel de impacto Alto, Muy alto y Crítico.

Cuarto. La resolución de 26 de enero de 2018, de la Dirección General de Telecomunicaciones y Sociedad de la Información, por la que se establecen normas sobre integración en el Centro de Seguridad TIC AndalucíaCERT requiere que todos los organismos y entidades comprendidos en el ámbito de aplicación del Decreto 1/2011, de 11 de enero, se integren en el grupo atendido de AndalucíaCERT, lo que les dotará de coordinación en materia de detección y respuesta a incidentes de seguridad TIC.

Quinto. Dicha coordinación requiere el establecimiento de procedimientos propios en cada organismo que definan las vías de comunicación, los roles y las tareas asociadas a la respuesta a incidentes de seguridad TIC.

Por todo lo anterior, se hace necesario el desarrollo en este sentido de la Política de Seguridad de las Tecnologías de la Información y Comunicaciones en la Administración de la Junta de Andalucía.

00139931

FUNDAMENTOS DE DERECHO

Primero. Es competente para dictar esta Resolución en este ámbito la Dirección General de Telecomunicaciones y Sociedad de la Información que, en virtud del Decreto 210/2015, de 14 de julio, por el que se regula la estructura orgánica de la Consejería de Empleo, Empresa y Comercio, ostenta las atribuciones de coordinación y ejecución de las políticas de seguridad de los sistemas de Información y telecomunicaciones de la Administración de la Junta de Andalucía.

Segundo. Las directrices en materia de seguridad TIC en el ámbito de la Administración de la Junta de Andalucía, sus entidades instrumentales y 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 se establecen 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 (modificado por el Decreto 70/2017, de 6 de junio).

Tercero. Por su parte, la 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, articula el desarrollo de dicha Política mediante 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.

Cuarto. Entre los ámbitos de desarrollo que establece dicha Orden de 9 de junio de 2016 está 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.

Vistos los antecedentes de hecho, los fundamentos de derecho y las demás normas de general aplicación, esta Dirección General de Telecomunicaciones y Sociedad de la Información, en uso de las atribuciones que tiene conferidas,

R E S U E L V E

Primero. Los organismos y entidades comprendidos en el ámbito de aplicación del Decreto 1/2011, de 11 de enero deberán adoptar las siguientes medidas en el ámbito de la gestión de incidentes de seguridad TIC:

1. Procedimiento de gestión de incidentes: los organismos y entidades dispondrán de un procedimiento alineado con lo dispuesto en los controles op.exp.7 (Gestión de incidentes) y op.exp.9 (Registro de la gestión de incidentes) del Esquema Nacional de Seguridad (apartados 4.3.7 y 4.3.9 del Anexo II) y con la guía CCN-STIC 817 (Esquema Nacional de Seguridad. Gestión de ciberincidentes) que incluirá, al menos: roles, mecanismos de detección, mecanismos de notificación (interna y externa), criterios de clasificación, mecanismos de registro, mecanismos de comunicación a partes interesadas y tareas de análisis, resolución y cierre.

2. Roles en gestión de incidentes: los roles se alinearán con los reflejados en la guía CCN-STIC 801 (Esquema Nacional de Seguridad. Responsabilidades y funciones). Se informará al Responsable de Seguridad del organismo o entidad y al Responsable del Sistema afectado de los incidentes (como mínimo de aquellos de nivel de impacto Alto, Muy Alto y Crítico) y de las acciones para su tratamiento.

3. Canales de notificación interna de incidentes de seguridad TIC: los organismos y entidades establecerán canales para la notificación de incidentes de seguridad TIC

00139931

por parte de su personal. Estas notificaciones serán recibidas y tratadas por el personal designado en el organismo o entidad para la gestión de incidentes.

4. Canales de notificación externa de incidentes de seguridad TIC: los organismos y entidades establecerán canales para la notificación de incidentes de seguridad desde el exterior. Como mínimo, se recibirán notificaciones por parte de AndalucíaCERT, y los canales estarán alineados con las directrices que se establezcan para dicha comunicación. Las notificaciones procedentes de AndalucíaCERT serán recibidas y tratadas por el personal designado en el organismo o entidad para la gestión de incidentes.

5. Registro de incidentes: los organismos y entidades mantendrán un registro de los incidentes y las tareas realizadas para su gestión incluyendo, al menos: información sobre la notificación inicial; actuaciones de emergencia adoptadas; modificaciones del sistema derivadas del incidente y evidencias que pudieran sustentar, en su caso, acciones legales o disciplinarias. La información sobre el incidente será tratada con la debida confidencialidad, tanto en lo relativo a los hechos como a los datos de la notificación.

6. Comunicación de incidentes: los organismos y entidades comunicarán los incidentes de nivel de impacto Alto, Muy Alto y Crítico a las partes interesadas (Responsables de la Información y/o del Servicio afectados, al menos) y al Comité de Seguridad TIC del organismo o entidad.

El cumplimiento de lo dispuesto en los artículos 36 y 37 del Real Decreto 3/2010, de 8 de enero, y desarrollado por la Instrucción Técnica de Seguridad de Notificación de Incidentes de Seguridad, acerca de la notificación al CCN de incidentes de nivel de impacto Alto, Muy alto y Crítico (según la clasificación de la guía CCN-STIC 817), se realizará a través de AndalucíaCERT.

Para la comunicación obligatoria de incidentes de seguridad a autoridades de control que sea requerida por otras normativas (protección de datos personales, protección de infraestructuras críticas…), mientras no se desarrollen directrices específicas en el ámbito de la Junta de Andalucía, los organismos y entidades utilizarán los canales que establezcan las correspondientes autoridades de control.

7. Concienciación y difusión: los organismos y entidades realizarán acciones de concienciación entre su personal abarcando, al menos, las responsabilidades que la normativa asigna en materia de seguridad, los conceptos básicos sobre incidentes de seguridad y los mecanismos de notificación interna.

8. Comunicación entre organismos y entidades de incidentes y medidas adoptadas: los incidentes detectados que afecten o provengan de otro organismo o entidad, y las posibles medidas de bloqueo o restricción que se adopten para su gestión, se notificarán a dicho organismo o entidad a través de AndalucíaCERT.

9. Colaboración con AndalucíaCERT: los organismos y entidades atenderán las consultas y peticiones que se realicen desde AndalucíaCERT para el diagnóstico, triaje y evaluación de peligrosidad e impacto de incidentes y vulnerabilidades.

10. Recolección y custodia de evidencias: si como parte de la gestión del incidente se recolectan evidencias con vistas a la realización de acciones legales o disciplinarias, los procesos de adquisición y custodia de las mismas se realizarán garantizando su validez jurídica.

11. Denuncias: en caso de que se considere que un incidente pueda ser constitutivo de delito, y proceda por tanto interponer denuncia policial, los organismos y entidades seguirán el protocolo de actuación que determinen los centros directivos con atribuciones al respecto.

Segundo. La presente Resolución surtirá efectos el día siguiente al de su publicación en el Boletín Oficial de la Junta de Andalucía.

Sevilla, 13 de julio de 2018.- El Director General, Manuel Ortigosa Brun.

00139931

ANEXO I

GLOSARIO

Activo TIC: Componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización.

CERT, CSIRT: Organización especializada en responder inmediatamente a incidentes relacionados con la seguridad de las redes o los equipos. También publica alertas sobre amenazas y vulnerabilidades de los sistemas. En general tiene como misiones elevar la seguridad de los sistemas de los usuarios y atender a los incidentes que se produzcan. Siglas inglesas correspondientes a Computer Emergency Response Team/Computer Security Incident Response Team.

Grupo atendido: Comunidad a la que presta servicios un CERT.

Incidente de seguridad: Suceso inesperado o no deseado con consecuencias en detrimento de la seguridad del sistema de información.

Nivel de impacto: Consecuencias de un incidente sobre las funciones de la organización, sus activos o los individuos afectados.

Responsable de la Información (Real Decreto 3/2010, art. 10): Persona que tiene la potestad de establecer los requisitos de la información tratada.

Responsable del Servicio (Real Decreto 3/2010, art. 10): Persona que tiene la potestad de establecer los requisitos de los servicios prestados.

Responsable de Seguridad (Real Decreto 3/2010, art. 10; Decreto 1/2011 modificado por Decreto 70/2017, art. 11): Persona que determina las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios.

Responsable del Sistema (Real Decreto 3/2010, art. 10): Persona que se encarga de la prestación de los servicios y, de la explotación del sistema de información.

00139931