

3. Otras disposiciones

CONSEJERÍA DE EMPLEO, EMPRESA Y COMERCIO

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.

Vistas las consideraciones aprobadas en el Comité de Seguridad TIC de la Junta de Andalucía en la reunión celebrada el día 2 de noviembre de 2017, y en base a 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 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), indica en su artículo 12 que la Consejería competente en materia de coordinación y ejecución de las políticas de seguridad de los sistemas de información y telecomunicaciones desarrollará acciones centralizadas de prevención, detección y respuesta a incidentes en el ámbito de la Administración de la Junta de Andalucía a través del centro especializado AndalucíaCERT.

Tercero. El centro de seguridad TIC AndalucíaCERT fue creado en 2010 y desde entonces viene prestando a su grupo atendido los servicios de detección y respuesta a incidentes de seguridad, monitorización de eventos de seguridad, análisis de vulnerabilidades, difusión de contenidos y alerta temprana de amenazas. Está en estudio la incorporación de nuevos servicios.

Cuarto. En el año 2016 AndalucíaCERT gestionó y coordinó la respuesta a más de 3.400 incidentes de seguridad TIC y desde su creación hasta finales de 2016 ha atendido aproximadamente 9.300, con incrementos anuales continuos, entre el 28 y el 57 por ciento. Algunos de los incidentes gestionados han implicado a múltiples organismos y entidades adscritos a la Red Corporativa de Telecomunicaciones de la Junta de Andalucía.

Quinto. Ante el crecimiento en el número y la peligrosidad de los incidentes, el Comité de Seguridad TIC de la Junta de Andalucía aprobó en la reunión celebrada el día 2 de noviembre de 2017 el carácter obligatorio para todos los organismos y entidades incluidos en el ámbito subjetivo de aplicación del Decreto 1/2011, de 11 de enero, para formar parte del grupo atendido de AndalucíaCERT.

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.

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.

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 integrarse en el grupo atendido de AndalucíaCERT siguiendo el procedimiento de adhesión vigente, que puede ser solicitado a través del correo electrónico consultas.cert@juntadeandalucia.es.

Segundo. Como parte del procedimiento de adhesión los organismos y entidades deberán suministrar información sobre sus activos TIC, la valoración de los mismos y los puntos de contacto para la notificación y gestión de incidentes de seguridad que les afecten.

Tercero. Será responsabilidad de los organismos y entidades mantener actualizada dicha información ante cambios en su personal, en sus activos TIC o en la valoración de éstos.

Cuarto. Esta obligación sólo se aplicará a los servicios que se ofrezcan desde AndalucíaCERT de forma gratuita.

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

Sevilla, 26 de enero de 2018.- El Director General, Manuel Ortigosa Brun.

A N E X O

G L O S A R I O

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

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.

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

Valoración: Estimación de la importancia relativa de un activo, determinada por su propietario.

Puntos de contacto: Interlocutores del grupo atendido de un CERT que pueden solicitar los servicios del mismo y que reciben notificaciones de incidentes y otras comunicaciones.