ACUERDO DE 9 DE OCTUBRE DE 2013, DEL PLENO DEL CONSEJO AUDIOVISUAL DE ANDALUCÍA, POR EL QUE SE APRUEBA LA POLÍTICA DE SEGURIDAD EN LOS SISTEMAS DE INFORMACIÓN

1.- De acuerdo con el artículo 131 de la Ley Orgánica 2/2007, de 19 de marzo, de reforma del Estatuto de Autonomía para Andalucía, el Consejo Audiovisual es la autoridad audiovisual independiente encargada de velar por el respeto de los derechos, libertades y valores constitucionales y estatutarios en los medios audiovisuales, tanto públicos como privados, en Andalucía, así como por el cumplimiento de la normativa vigente en materia audiovisual y de publicidad. Su composición, competencia y funcionamiento se regula en la Ley 1/2004, de 17 de diciembre, de creación del Consejo Audiovisual de Andalucía y en el Reglamento Orgánico y de Funcionamiento del Consejo Audiovisual de Andalucía, aprobado por Decreto 219/2006, de 19 de diciembre.

2.- El Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad (RDENS) en el ámbito de la Administración Electrónica, da cumplimiento a lo previsto en el artículo 42 de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos. Su finalidad es la creación de las condiciones necesarias de confianza en el uso de los medios electrónicos, a través de medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones, y los servicios electrónicos, que permita a los ciudadanos y a las Administraciones públicas, el ejercicio de derechos y el cumplimiento de deberes a través de estos medios.

3.- De conformidad con lo dispuesto en el artículo 14 del RDENS, todos los órganos superiores de las Administraciones Públicas deberá disponer formalmente de su política de seguridad, que deberá ser aprobada por el titular del órgano superior correspondiente.

El Esquema Nacional de Seguridad define la seguridad de la información como la capacidad de las redes o de los sistemas de información de resistir, con un determinado nivel de confianza, los accidentes o acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos y de los servicios que las redes y sistemas mencionados ofrecen o hacen accesibles.

Respecto a los sistemas afectados, el artículo 5 del RDENS indica que la seguridad se entiende como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con los sistemas de información.

En este sentido, el anexo IV del RDENS define los sistemas de información como los conjuntos organizado de recursos para que la información se pueda recoger, almacenar, procesar o tratar, mantener, utilizar, compartir, distribuir, poner a disposición, presentar o transmitir.

Por lo tanto, el Esquema Nacional de Seguridad, se aplica esencialmente a los sistemas de información que soportan la actividad administrativa, la actividad interadministrativa y las relaciones con los ciudadanos.

Para cumplir con el Esquema Nacional de Seguridad resulta necesario, aplicar un conjunto de medidas identificadas en el anexo II de la norma, considerando los activos del sistema de los información, la categoría de los sistemas y las decisiones que se adopten para gestionar los riesgos identificados, de forma integrada, en su caso, con la reglamentación de seguridad de protección de datos de carácter personal.

4.- El Consejo Audiovisual de Andalucía asume el compromiso de controlar sus riesgos de seguridad, así como dar cumplimiento a la legislación y normas internas vigentes bajo un proceso de mejora continua mediante la implementación en espiral de un Sistema de Gestión de Seguridad de la Información (SGSI), ajustado a los marcos metodológicos vigentes (MAGERIT, Metodología de Análisis y Gestión de Riesgos para la Seguridad de los Sistemas de Información del Ministerio para las Administraciones Públicas; ISO/IEC 27001 y 27002) con el fin de estudiar y actuar sobre el nivel de exposición de los sistemas de información e infraestructuras de la organización, adoptando una perspectiva de estudio de riesgos (art. 6 RDENS), y abordando los aspectos de seguridad necesarios para la protección y funcionamiento de estos sistemas.

A la vista de lo anterior, de acuerdo con el artículo 9.1 de la Ley 1/2004, de 17 de diciembre, de creación del Consejo Audiovisual de Andalucía y en el Reglamento Orgánico y de Funcionamiento del Consejo Audiovisual de Andalucía, aprobado por el Decreto 219/2006, de 19 de Diciembre, por el que se establece la estructura orgánica del Consejo Audiovisual de Andalucía, el Pleno del Consejo Audiovisual de Andalucía,

ACUERDA

PRIMERO: Aprobar la Política de Seguridad en los Sistemas de Información del Consejo Audiovisual de Andalucía que se incorpora como **ANEXO**.

Sevilla a 9 de octubre de 2013

LA PRESIDENTA DEL CONSEJO AUDIOVISUAL

DE ANDALUCÍA

Fdo: Emelina Fernández Soriano

ANEXO : POLÍTICA DE SEGURIDAD EN LOS SISTEMAS DE INFORMACIÓN DEL CONSEJO AUDIOVISUAL DE ANDALUCÍA.

1.- INTRODUCCIÓN

El presente documento tiene por objeto establecer el marco de gestión de la seguridad de la información según lo establecido en el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de la Seguridad en el ámbito de la administración electrónica, reconociendo así como activos estratégicos la información y la política de seguridad del CAA, con la finalidad de garantizar la calidad de la información y la prestación continuada de los servicios del CAA.

Los sistemas TIC (Tecnología de Información y Comunicaciones) deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a los daños accidentales o deliberados que puedan afectar a la confidencialidad, integridad, autenticidad, trazabilidad y disponibilidad de la información tratada o los servicios prestados.

2.- MARCO NORMATIVO

Esta política de seguridad que se pone en práctica se fundamenta, sin carácter exhaustivo, en las siguientes normas de rango legal y reglamentario:

- Ley 1/2004, de 17 de diciembre, de creación del CAA
- Decreto 219/2006, de 19 de diciembre, por el que se aprueba el Reglamento Orgánico y de funcionamiento del CAA.
- Ley 30/1992, de 26 de noviembre, de régimen jurídico de las administraciones públicas y del procedimiento administrativo común.
- Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal y sus normas de desarrollo.
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
- La Resolución de 27 de Septiembre 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.
- Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos.
- Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.
- Real Decreto 3/2010, de 8 de enero, que regula el Esquema Nacional de Seguridad (ENS) en el ámbito de la Administración Electrónica.
- Ley 7/2011, de 3 noviembre, de Documentos, Archivos y Patrimonio Documental de Andalucía.

3.- ORGANIZACIÓN DE LA SEGURIDAD

La organización de la seguridad queda establecida mediante la identificación y definición de los diferentes roles que a continuación se relacionan, con la funciones y responsabilidades establecidas en la Guía de Seguridad CCN-STIC-801, de febrero de

2011, NIPO:075-11-053-3, elaborada y difundida para el mejor cumplimiento de lo establecido en el Esquema Nacional de Seguridad, de conformidad con lo establecido en el artículo 29 del Real Decreto 3/2010.

3.1 Responsables

La estructura de la organización de la seguridad TIC del CAA está integrada por:

-El *Responsable de la Información (RINFO)* que será el Pleno del CAA.

-El *Responsable de los Servicios (RSERV)* que será el Pleno del CAA.

-El *Responsable de Seguridad (RSEG) que* será la persona titular de la Secretaría General del CAA.

-El *Responsable de los Sistemas automatizados (RSIS) y Administrador de la Seguridad TIC (ASS)* que será la persona titular del Gabinete de Telecomunicaciones.

Junto a ellos, los responsables de gestión del personal y de la gestión física de las instalaciones implantarán las medidas de seguridad que le competan dentro de las determinadas por el Responsable de la Seguridad de la Información, e informarán a éste de su grado de implantación, eficacia e incidentes.

3.2 Funciones

El Responsable de la Información y de los Servicios, además de ejercer las funciones previstas en los apartados 5.1 y 5.2 de la Guía de Seguridad CCN-STIC-801 y atendiendo las propuestas del Responsable de Seguridad y de los responsables de las distintas áreas:

-Aprobará las políticas generales de seguridad, así como definir las normas, procedimientos e instrucciones técnicas.

-Velará por el uso que se haga de una cierta información y de su protección, prestando especial atención a todo lo referente a errores y negligencias así como a los incidentes de confidencialidad o de integridad.

-Proveerá dentro del marco presupuestario, los recursos para la seguridad.

El Responsable de Seguridad, además de ejercer las funciones previstas en el apartado 6 y el Anexo A de la Guía de Seguridad CCN-STIC-801 y atendiendo las propuestas del Responsable de los Sistemas automatizados y Administrador de Seguridad TIC y de los responsables de las distintas áreas:

-Velará por el cumplimiento de la legislación y normativa vigente en materia de seguridad así como de todo el esquema organizativo, roles y funciones que exige el ENS en los sistemas a los que se aplica.

-Controlará los niveles de riesgo definidos y aceptados.

El Responsable de los Sistemas automatizados y Administrador de Seguridad TIC además de ejercer las funciones previstas en los apartados 7.1 y 8 y en el Anexo A de la Guía de Seguridad CCN-STIC-801:

-Comunicará a los terceros que colaboren en la explotación de los sistemas encuadrados dentro del ENS las categorizaciones propias de dichos sistemas, para que las tengan en cuenta, incorporando estos requisitos a su propio plan de adecuación o a su propia declaración de conformidad.

-Realizará el seguimiento de auditorías e indicadores de seguridad y velará por el cumplimiento de las indicaciones que de las mismas resulten.

-Realizará revisiones periódicas del Sistema de Gestión de la Seguridad de la Información (SGSI), del Documento de Seguridad (DS), del Sistema de Gestión y Evaluación de la Calidad en las Tecnologías de la Información y Comunicaciones (SGEC-TIC) y de toda la documentación referente a materia de seguridad y calidad.

3.3 Procedimiento de designación

El Pleno del CAA podrá revisar los nombramientos de los Responsables.

En caso de conflictos o diferentes interpretaciones de esta política se recurrirá al Pleno del CAA.

4.- DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Se consideran instrumentos básicos para el desarrollo de la presente política de seguridad:

-El Documento de Seguridad como ordenamiento normativo de obligado cumplimiento en cuanto a medidas de seguridad.

-El Sistema de Gestión de Seguridad de la Información (SGSI) que basado en el estudio de los riesgos, se establece para crear, implementar, hacer funcionar, supervisar, revisar, mantener y mejorar la seguridad de la información. Incluye la estructura organizativa, las políticas, las actividades de planificación, las responsabilidades, las prácticas, los procedimientos, los procesos y los recursos. Permite conocer los niveles de riesgo y planificar su minimización. Previsto en el R.D. 3-2010, Anexo III, Auditoría de seguridad apartado 1 f) y en la guía CCN-STIC-802 apartado 25.

-El Sistema de Gestión y Evaluación de la Calidad en las Tecnologías de la Información y Comunicaciones (SGEC-TIC) como vértice del trinomio Funcionalidad-Calidad-Seguridad, siendo este último un elemento más a exigir en las relaciones entre los distintos actores con responsabilidades en los sistemas.

5.- MEDIDAS DE OBLIGADO CUMPLIMIENTO PARA LA ORGANIZACIÓN

Todas las medidas en materia de seguridad contempladas en el Esquema Nacional de Seguridad para los sistemas afectados según su categorización, serán aplicadas y de obligado cumplimiento para toda la organización. En particular se adoptarán:

-Medidas de Protección de las instalaciones e infraestructuras, para lo cual se proveerán los recursos necesarios a tal efecto.

-Gestión de personal, fundamentada en la profesionalización (art. 15 ENS), junto con la formación e información de naturaleza iterativa y atendiendo siempre al momento tecnológico en los aspectos de seguridad en las TIC.

-Protección de activos, que permiten la existencia de servicios y atención al ciudadano.

-Protección de la información, según marca la LOPD.

-Protección de las aplicaciones, teniendo especial atención al desarrollo, a la aceptación y puesta en servicio.

-Generación y actualización de la documentación existente en materia de seguridad bajo un gestor documental imbricado con el SGSI y su normativa de uso, basada en el principio de mejora continua del proceso de seguridad (art. 26 ENS) y una continua reevaluación de la misma (art. 9 ENS).

Todas estas actuaciones, así como cualquier otra medida en este ámbito, deberán de ser enmarcadas en un conjunto programático o línea de actuación, evitándose el carácter puntual de las mismas y permitiéndose así, su supervisión, control, métrica y análisis de impacto en los aspectos de funcionalidad y continuidad del servicio.

6.- MEDIDAS DE OBLIGADO CUMPLIMIENTO PARA EL PERSONAL.

Todas las personas que prestan sus servicios en las distintas áreas del Consejo Audiovisual de Andalucía deberán:

-Conocer y cumplir las obligaciones relativas al uso correcto de los recursos informáticos y documentales, recogidas en la Resolución de 27 de Septiembre de 2004 de la Secretaría General para la Administración Pública (Manual del Empleado Público), así como en las demás normas sobre esta materia.

-Conocer los ficheros con datos de carácter personal declarados por el Consejo. Además, deberán cumplir cuantas medidas sean adoptadas por los titulares de los Órganos responsables de dichos ficheros, tanto en lo relativo a la seguridad de los datos como en lo referente al cumplimiento de aquellas otras medidas dirigidas a hacer efectivas las garantías, derechos y obligaciones contemplados en la normativa de protección de datos vigente.

-Asumir el deber de colaboración con la Organización en el interés de que no se produzcan alteraciones o violaciones de estas reglas y dará cuenta inmediatamente de todas las incidencias de que tenga conocimiento al inmediato superior. El incumplimiento de esta resolución podrá dar lugar a la exigencia de responsabilidad disciplinaria conforme a los procedimientos legales y demás normas aplicables.

7.- ENTRADA EN VIGOR, DIFUSIÓN Y REVISIÓN DE LA POLÍTICA

Esta política de seguridad es efectiva desde el 9 de octubre de 2013, fecha de su aprobación por el Pleno del CAA.

La misma se difundirá, por los titulares de las distintas áreas, entre todo el personal que preste sus servicios en el Consejo.

Esta política podrá ser revisada por el Pleno, con el fin de asegurar que se adecua a la estrategia y necesidades de la organización.