3. Otras disposiciones

CÁMARA DE CUENTAS DE ANDALUCÍA

Resolución de 8 de mayo de 2018, del Presidente de la Cámara de Cuentas de Andalucía, por la que se publica el Acuerdo de Pleno, por el que se aprueban las normas que regulan la Política de Seguridad de la Información en el ámbito de la administración electrónica en la Cámara de Cuentas de Andalucía.

La Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, establece que las Administraciones Públicas se relacionarán entre sí y con sus órganos, organismos públicos y entidades vinculados o dependientes a través de medios electrónicos. Dichos medios deben asegurar la interoperabilidad y seguridad de los sistemas y soluciones adoptadas y garantizarán la protección de los datos de carácter personal.

Por su parte, la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, recoge en su artículo 13, sobre derechos de las personas en sus relaciones con las Administraciones Públicas, el relativo a la protección de datos de carácter personal.

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, modificado parcialmente por el Real Decreto 951/2015, de 23 de octubre, tiene por objeto determinar la política de seguridad en la utilización de medios electrónicos en su ámbito de aplicación, sus principios básicos y los requisitos mínimos que permitan una protección adecuada de la información.

El artículo 11 del citado Real Decreto 3/2010, de 8 de enero, exige que todos los órganos superiores de las Administraciones públicas dispongan formalmente de su política de seguridad, que se aprobará por el titular del órgano superior correspondiente.

El presente Acuerdo, por tanto, tiene la finalidad de aprobar la Política de Seguridad de la Información de la Cámara de Cuentas de Andalucía, así como establecer la estructura organizativa para definirla, implantarla y gestionarla.

El Pleno de la Cámara de Cuentas de Andalucía en su sesión de 8 de mayo de 2018, ha adoptado un acuerdo aprobando las normas que regulan la Política de Seguridad de la Información en el ámbito de la administración electrónica en la Cámara de Cuentas de Andalucía, acuerdo que esta Presidencia hace público, en el ejercicio de las atribuciones que le confiere el artículo 22.a) del citado Reglamento de Organización y Funcionamiento.

Acuerdo de Pleno, de 8 de mayo de 2018, por el que se aprueban las normas que regulan la Política de Seguridad de la Información en el ámbito de la administración electrónica en la Cámara de Cuentas de Andalucía.

La Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, establece que las Administraciones Públicas se relacionarán entre sí y con sus órganos, organismos públicos y entidades vinculados o dependientes a través de medios electrónicos. Dichos medios deben asegurar la interoperabilidad y seguridad de los sistemas y soluciones adoptadas y garantizarán la protección de los datos de carácter personal.

Por su parte, la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, recoge en su artículo 13, sobre derechos de las personas en sus relaciones con las Administraciones Públicas, el relativo a la protección de datos de carácter personal.

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, modificado parcialmente por el Real Decreto 951/2015, de 23 de octubre, tiene por objeto determinar la política de seguridad en la utilización de medios electrónicos en su ámbito de aplicación, sus

00136118

principios básicos y los requisitos mínimos que permitan una protección adecuada de la información.

El artículo 11 del citado Real Decreto 3/2010, de 8 de enero, exige que todos los órganos superiores de las Administraciones públicas dispongan formalmente de su política de seguridad, que se aprobará por el titular del órgano superior correspondiente.

El presente acuerdo, por tanto, tiene la finalidad de aprobar la Política de Seguridad de la Información de la Cámara de Cuentas de Andalucía, así como establecer la estructura organizativa para definirla, implantarla y gestionarla.

Artículo 1. Objeto.

Uno. El presente acuerdo tiene por objeto aprobar la Política de Seguridad de la Información (en adelante PSI) en el ámbito de la administración electrónica de la Cámara de Cuentas de Andalucía, así como establecer la estructura organizativa para definirla, implantarla y gestionarla.

Dos. La finalidad de la PSI 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 ejercer sus derechos y el cumplimiento de deberes, aportando un lenguaje común para facilitar la interacción de las Administraciones Públicas y los ciudadanos.

Tres. La PSI afectará a la información tratada por medios electrónicos y a la información en soporte papel que la Cámara de Cuentas de Andalucía gestiona en el ámbito de sus competencias.

Cuatro. La información que contenga datos de carácter personal se verá afectada por la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y su normativa de desarrollo mientras estén vigentes y por el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

Cinco. La información producida, conservada o reunida, cualquiera que sea su soporte, susceptible de formar parte del patrimonio documental se verá afectada por la Ley 7/2011, de 3 de noviembre, de Documentos, Archivos y Patrimonio Documental de Andalucía.

Seis. La información contenida en los sistemas de información, en el ámbito de la administración electrónica, queda regulada por el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad.

Siete. La PSI será de obligado cumplimiento para todo el personal que acceda tanto a los sistemas de información como a la propia información que sea gestionada por la Cámara de Cuentas de Andalucía, con independencia de cuál sea su destino o adscripción.

Artículo 2. Ámbito de aplicación.

El ámbito de aplicación del Presente documento de Política de Seguridad es el de los sistemas de información gestionados por la Cámara de Cuentas de Andalucía.

Artículo 3. Principios de la seguridad de la información.

Uno. Los principios básicos son directrices fundamentales de seguridad que han de tenerse siempre presentes en cualquier actividad relacionada con el uso de los activos de información. Se establecen los siguientes:

a) Alcance estratégico: La seguridad de la información debe contar con el compromiso y apoyo de todos los niveles directivos de forma que pueda estar coordinada e integrada con el resto de iniciativas estratégicas de la Cámara de Cuentas para conformar un todo coherente y eficaz.

00136118

b) Responsabilidad diferenciada: En los sistemas de información se diferenciará el responsable de la información, que determina los requisitos de seguridad de la información tratada; el responsable del servicio, que determina los requisitos de seguridad de los servicios prestados; el responsable del sistema, que tiene la responsabilidad sobre la prestación de los servicios y el responsable de seguridad, que determina las decisiones para satisfacer los requisitos de seguridad.

c) Seguridad integral: La seguridad se entenderá como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con el sistema. La seguridad de la información debe considerarse como parte de la operativa habitual, estando presente y aplicándose desde el diseño inicial de los sistemas de información.

d) Gestión de Riesgos: El análisis y gestión de riesgos es parte del proceso de seguridad. La gestión de riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. La reducción de estos niveles se realizará mediante el despliegue de medidas de seguridad, que establecerá un equilibrio entre la naturaleza de los datos y los tratamientos, el impacto y la probabilidad de los riesgos a los que estén expuestos y la eficacia y el coste de las medidas de seguridad. Al evaluar el riesgo en relación con la seguridad de los datos, se deben tener en cuenta especialmente los riesgos que se derivan del tratamiento de los datos personales.

e) Proporcionalidad: El establecimiento de medidas de protección, detección y recuperación deberá ser proporcional a los potenciales riesgos y a la criticidad y valor de la información y de los servicios afectados.

f) Mejora continua: Las medidas de seguridad se reevaluarán y actualizarán periódicamente para adecuar su eficacia. La seguridad de la información será atendida, revisada por personal cualificado y dedicado.

g) Seguridad por defecto: Los sistemas de información desde su diseño deben configurarse para que garanticen un grado suficiente de seguridad por defecto.

Dos. Las directrices fundamentales de seguridad se concretan en un conjunto de principios particulares y responsabilidades específicas, que se configuran como objetivos instrumentales de la PSI. Se establecen los siguientes:

a) Protección de datos de carácter personal: Se adoptarán las medidas técnicas y organizativas necesarias para atender los riesgos generados por el tratamiento de acuerdo a lo exigido por el citato Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016.

b) Gestión de activos de información: Los activos de información estarán inventariados, categorizados y asociados a un responsable.

c) Seguridad ligada a las personas: Se implantarán los mecanismos necesarios para que cualquier persona que acceda, o pueda acceder a los activos de información, conozca sus responsabilidades y de este modo se reduzca el riesgo derivado de un uso indebido de dichos activos.

d) Seguridad física: Los equipos de información se ubicarán en zonas seguras, protegidas por controles de acceso físicos adecuados a su nivel de criticidad. Los sistemas y los activos de información que contienen dichas áreas estarán suficientemente protegidos frente a amenazas físicas, ambientales y de acceso.

e) Seguridad en la gestión de las comunicaciones y operaciones: Se establecerán los procedimientos necesarios para lograr una adecuada gestión de la seguridad, operación y actualización de las Tecnologías de la Información y Comunicaciones. La información que circule en redes de comunicaciones deberá ser adecuadamente protegida, teniendo en cuenta su nivel de sensibilidad y criticidad.

f) Control de acceso: El acceso a los activos de información será limitado y estará controlado por mecanismos de identificación y autenticación. Además, quedará registrada la utilización del sistema para asegurar la trazabilidad del acceso y auditar su uso adecuado, conforme a la actividad de la organización.

00136118

g) Adquisición, desarrollo y mantenimiento de los sistemas de información: La seguridad de los sistemas estará presente en todas las fases del ciclo de vida de los sistemas de información, garantizando su seguridad por defecto.

h) Gestión de incidentes: Se implantarán los mecanismos apropiados para la correcta identificación, registro y resolución de los incidentes de seguridad.

i) Gestión de la continuidad: Se implantarán los mecanismos apropiados para asegurar la disponibilidad de los sistemas de información y mantener la continuidad de sus procesos de negocio, de acuerdo a las necesidades de nivel de servicio de sus usuarios.

j) Cumplimiento: Se adoptarán las medidas técnicas, organizativas y procedimentales necesarias para el cumplimiento de la normativa legal vigente en materia de seguridad de la información.

Artículo 4. Estructura organizativa.

La estructura organizativa para gestionar, mantener, actualizar y hacer cumplir la PSI de la Cámara de Cuentas de Andalucía, está compuesta por los siguientes agentes:

a) Comisión de seguridad de la información.
b) Comisión responsable de la seguridad de la información.
c) Responsable de la información.
d) Responsable del servicio.
e) Responsable de la seguridad.
f) Grupos de trabajo.

Artículo 5. Aspectos organizativos de la seguridad.

A nivel de organización interna, el objeto de este procedimiento es la gestión de la seguridad de la información dentro de la organización, así mismo, y en relación con los terceros que intervienen será necesario mantener la seguridad de la información de la organización y de los dispositivos de procesado que son objeto de acceso, tratamiento, comunicación o gestión de terceros.

Artículo 6. Comisión de seguridad.

Uno. Adscrito a la Presidencia de la Cámara de Cuentas de Andalucía, se crea la Comisión de Seguridad, como órgano colegiado de los previstos en el artículo 20.2 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, que debe promover la seguridad en la Organización por medio de un compromiso apropiado y de la adjudicación de los recursos adecuados, así como de la normativa orientada a la adaptación de los sistemas de información y bases de datos La Comisión de Seguridad de la Información es un foro de gestión que define la política de seguridad, su revisión y establece los riesgos de los activos de la empresa a la ley orgánica de protección de datos.

Esta comisión estará formada al menos por los siguientes miembros:

I. Un Consejero de la Cámara de Cuentas de Andalucía, presidirá esta comisión.
II. Titular de la Secretaría General de la Cámara de Cuentas de Andalucía.
III. Titular de Coordinación de Secretaría General y Jefa del Gabinete Jurídico de la Cámara de Cuentas de Andalucía.
IV. Dos Coordinadores de Departamento designados por Presidente de Cámara de Cuentas de Andalucía a propuesta del Presidente de esta Comisión.
V. Titular del Servicio de Informática.
VI. El delegado de seguridad.
VII. El delegado de protección de datos.

Dos. Las funciones de la comisión de seguridad son:

a) Hacer propuestas de aprobación, estudio, análisis y divulgación de las estrategias, normativas y políticas de seguridad de la Cámara de cuentas de Andalucía.

b) Impulsar el cumplimiento de la PSI y su desarrollo normativo.

00136118

c) Apoyar la cooperación y colaboración con otras administraciones en materia de seguridad de la información.

d) Elaborar propuestas de modificación y actualización permanente de la Política de Seguridad del documento de seguridad y resto de normativa de seguridad que elabora el responsable de seguridad de la Cámara de Cuentas de Andalucía.

e) Proponer el inicio de la implantación del SGSI. (sistema de gestión seguridad de información).

f) Proponer la documentación que constituye el SGSI (sistema de gestión seguridad de información).

g) Velar por la difusión del PSI, promoviendo actividades de concienciación y formación en materia de seguridad.

h) Evaluar de forma periódica el grado de exposición a riesgos que afecten a los sistemas de información de Cámara de Cuentas de Andalucía.

i) Proponer y revisar las medidas y normativas orientadas a garantizar la adecuación de los sistemas de información, bases de datos, y procedimientos a lo establecido en la Ley Orgánica de Protección de Datos, y demás leyes, normas o procedimientos que sobre estas materias puedan los organismos competentes emitir en un futuro.

j) Proponer la aprobación del plan de auditoría y formación propuestos por el responsable de seguridad.

k) Resolver los conflictos de competencia que pudieran surgir entre los diferentes departamentos en materia de seguridad.

l) Coordinar la seguridad de la información en toda la Institución.

m) Se implantarán los mecanismos apropiados para correcta identificación, registro y resolución de incidentes de seguridad.

n) Se implantarán mecanismos apropiados para asegurar la disponibilidad de los sistemas de información y mantener la continuidad de sus procesos, de acuerdo con las necesidades de usuarios y nivel de servicio.

o) La Comisión de Seguridad de la Información ejercerá la coordinación en materia de seguridad informática. A tal efecto, la Comisión podrá convocar a las personas que estime oportunas para ejercer el seguimiento del grado de implantación de las normativas de seguridad de la información en su ámbito de aplicación, así como velar por el cumplimiento de las mismas.

p) El desarrollo, mantenimiento y gestión de los programas y políticas de seguridad corresponde a la Comisión de Seguridad de la Información.

Tres. El Comité de Seguridad se reunirá con carácter ordinario al menos una vez al año y con carácter extraordinario cuando lo decida su Presidente. En cuanto a su funcionamiento, se regirá, en todo lo previsto en el presente Acuerdo, por lo dispuesto en el Capítulo II, Sección 3.ª, del Título Preliminar de la Ley 40/2015, de 1 de octubre, que regula el funcionamiento de los órganos colegiados.

Artículo 7. Comisión responsable de seguridad.

Uno. Las actividades relativas a la seguridad de la información deben ser coordinadas entre los representantes de las diferentes partes de la organización con sus correspondientes roles y funciones. de trabajo. La coordinación en materia de seguridad de la información es tarea del Responsable del SGSI (sistema de gestión seguridad de información), supervisado por la Comisión de Seguridad de la Información. Este comité es eminentemente operativo y es el encargado de ejecutar y hacer el seguimiento de las actuaciones en materia de seguridad establezca la Cámara de Cuentas de Andalucía.

Esta comisión estará formada al menos por los siguientes miembros:

I. Titular de la jefatura de servicio de informática que presidirá la Comisión de Seguridad de la Información.

II. Titulares de los Departamentos de Explotación y Desarrollo del servicio de informática.

00136118

III. Dos Coordinadores de Departamento propuestos por la Comisión de Seguridad, y designados por el Presidente de Cámara de Cuentas de Andalucía.
IV. El delegado de protección de datos.
V. El delegado de seguridad.
VI. Este Comité contará con el asesoramiento de un Letrado.
Dos. Las funciones de la comisión responsable de seguridad son:
a) Implantación, desarrollo y mantenimiento del SGSI.
b) Analizar el cumplimiento de la Política de Seguridad de la Información y su desarrollo normativo.
c) Analizar las medidas de seguridad de la información y de los servicios electrónicos prestado por los sistemas de información.
d) Informar a la Comisión de Seguridad de la Información de las cuestiones e incidencias relevantes y del grado de consecución de los objetivos.
e) Propondrá los Planes de Mejora y solicitará la aprobación de las inversiones que posiblemente conlleven.
f) Definir y desarrollar un conjunto de procedimientos de seguridad y estándares que los soporten.
g) Ofrecer asesoramiento en todos los aspectos de la seguridad de la información.
h) Investigar todos los incidentes de seguridad que sucedan.
i) Desarrollar los programas de concienciación y formación en seguridad para los empleados de la empresa.
j) Análisis de riesgos.
k) Proyectos relacionados con la seguridad.
l) Auditorías.
m) Incorporación de requerimientos de seguridad de la información en contratos y acuerdos.
n) Estudiar las actividades de concienciación y formación en materia de seguridad.
o) Desarrollo de planes de continuidad de negocio en la organización.
Tres. La Comisión de Seguridad de la Información se reunirá con carácter ordinario con una frecuencia de dos veces al año y, con carácter extraordinario, cuando lo decida su presidente.

Artículo 8. Responsables de la información.
Los responsables de la información tienen la potestad, dentro de su ámbito de actuación y competencias, establecer los requisitos, en materia de seguridad, de la información que manejan. Si esta información incluye datos de carácter personal. Además, deberán tenerse en cuenta las medidas de seguridad que correspondan implantar atendidos los riesgos generados por el tratamiento de acuerdo a lo exigido por Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril 2016.
Las funciones del responsable de la información recaerán en la persona titular de la unidad administrativa que gestiona cada procedimiento administrativo, pudiendo una misma persona acumular las responsabilidades de la información de todos los procedimientos que se gestionen.

Artículo 9. Responsable del servicio.
Los Responsables del Servicio tienen la potestad, dentro de su ámbito de actuación y de sus competencias, de establecer los requisitos, en materia de seguridad, de los servicios. Si estos servicios incluyen datos de carácter personal, además deberán tenerse en cuenta las medidas de seguridad que corresponda implantar atendidos los riesgos generados por el tratamiento de acuerdo a lo exigido por el citato Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016.
Las funciones de Responsable del Servicio recaerán en la persona titular del órgano o unidad administrativa que gestione cada procedimiento administrativo, pudiendo una

00136118

misma persona acumular las responsabilidades del servicio de todos los procedimientos que gestione, sin que implique, en ningún caso, un aumento de las actuales dotaciones ni de las retribuciones de dichos efectivos por ningún concepto.

Artículo 10. Responsable de seguridad.

La Comisión responsable de seguridad toma las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios.

El ámbito de actuación se limitará única y exclusivamente a los sistemas de información y servicios de tecnologías de la información y de las comunicaciones que sean competencia y responsabilidad directa suya.

El jefe de informática tendrá el rol de administrador de la seguridad del sistema y tienen las funciones siguientes:

a) Verificar la aprobación de procedimientos operativos de seguridad.

b) Asegurar el cumplimiento de los controles de seguridad.

c) Supervisar instalaciones de hardware y software, sus modificaciones y mejoras para asegurar que la seguridad no está comprometida.

d) Supervisar la monitorización de la seguridad del sistema.

e) Informar a los responsables de seguridad de cualquier anomalía e incidencia.

f) Colaborar en la solución de incidentes de seguridad, desde su detección hasta su solución.

Artículo 11. Política de seguridad.

La Comisión de Seguridad de la Información/Dirección debe proponer el documento de Política de Seguridad de la Información de la entidad, publicarla y distribuirla a todos sus empleados, así como a terceras partes que puedan verse involucradas en la implementación del sistema.

La Política de Seguridad de la Información debe definir la seguridad de la información, su alcance, las responsabilidades asociadas y los principios de seguridad que deben seguirse por parte de los usuarios; debe revisarse a intervalos planificados o siempre que se produzcan cambios significativos, a fin de asegurar que se mantenga su idoneidad, adecuación y eficacia.

Artículo 12. Seguridad ligada al personal.

Las funciones y responsabilidades sobre la seguridad de la información, de acuerdo con la política de seguridad de la organización se documentarán. Se implantarán mecanismos necesarios para que cualquier persona conozca sus responsabilidades y se reduzca el riesgo derivado de un uso indebido.

Se establecerán normas de obligado cumplimiento para todo el personal con objeto de reducir riesgos asociados a los activos.

Artículo 13. Grupos de trabajo.

Se articularán grupos de trabajo para la realización de actividades que se estimen convenientes, tales como la elaboración de estudios, trabajos e informes.

Los grupos de trabajo estarán compuestos por el titular de la comisión de seguridad de la información, el delegado de seguridad y los responsables del mantenimiento del sistema y entre otras cuestiones les corresponden:

a) Elaborar estudios previos y propuestas de modificación del plan de seguridad.

b) Analizar el cumplimiento del plan de seguridad.

c) Coordinar la comunicación con el Centro Criptológico Nacional, Andalucía-Cert y Red Corporativa de la Junta de Andalucía.

d) Estudiar las medidas de concienciación y formación en materia de seguridad.

00136118

Artículo 14. Resolución de conflictos.

En caso de conflicto entre los diferentes responsables que componen la estructura organizativa de la PSI prevalecerá la decisión de la Comisión de Seguridad.

Artículo 15. Gestión de riesgos.

La gestión de riesgos debe realizarse de manera continua sobre el sistema de información. El servicio de informática es el encargado de realizar el preceptivo análisis de riesgos y se proponer el tratamiento adecuado.

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.

El análisis de riesgos deberá realizarse al menos una vez cada dos años, cuando cambie la información o los servicios prestados, cuando ocurra un incidente de seguridad y cuando se reporte una vulnerabilidad grave.

Artículo 16. Desarrollo normativo.

El cuerpo normativo sobre seguridad de la información se desarrollará por el Pleno de la Cámara de Cuentas de Andalucía a nivel de detalle técnico y obligatoriedad de cumplimento.

Artículo 17. Protección de datos de carácter personal.

En lo referente a los datos de carácter personal que sean objeto de tratamiento por parte de la Cámara de Cuentas de Andalucía, se adoptarán las medidas técnicas y organizativas que corresponda a lo expresado en el artículo 24.1 del Reglamento (UE) 2016/679.

Respecto a la protección de datos de carácter personal, el responsable del servicio asumirá las funciones de responsable del tratamiento.

En caso de conflicto entre los diferentes responsables, prevalecerán las mayores exigencias derivadas de la protección de datos de carácter personal.

Artículo 18. Terceros.

Cuando la Cámara de Cuentas de Andalucía requieran la participación de terceras partes, deberán identificarse los riesgos de la información que la organización va a dejar disponible, reduciendo el riesgo a un nivel aceptable, para ello, se pondrá en conocimiento del tercero la PSI que estará obligado a cumplir.

Las relaciones con terceros deben ser identificadas, aprobadas y recogidas por un contrato, que contenga las cláusulas de confidencialidad establecidas en el Documento de Seguridad, de manera que garantice el acceso a los sistemas de información.

Artículo 19. Formación y concienciación.

Se desarrollarán actividades formativas específicas orientadas a la concienciación y formación de los empleados, así como a la difusión entre los mismos de la Política de Seguridad y de su desarrollo normativo.

El Grupo de trabajo de seguridad de la información y los responsables de seguridad se encargarán de promover las actividades de formación y concienciación en materia de seguridad.

Artículo 20. Obligaciones de los usuarios.

a) Todos los usuarios de la Cámara de Cuentas de Andalucía, deberán conocer el documento de Política de Seguridad; para ello, se dispondrán los medios necesarios para su difusión, prestando especial atención a las nuevas incorporaciones.

b) Atenderán a una acción de concienciación en materia de seguridad relativa a las tecnologías de la información y comunicaciones.

00136118

c) Las personas con responsabilidad en la operación o administración de sistemas recibirán formación para el manejo seguro de los sistemas en la medida que la necesiten para realizar su trabajo. La formación será obligatoria antes de asumir su trabajo tanto si es su primera asignación como si se trata de un cambio.

Disposición Final.

El presente Acuerdo entrará en vigor el día siguiente al de su aprobación por el Pleno de la Cámara de Cuentas de Andalucía.

Disposición Derogatoria.

Quedan derogadas todas las disposiciones de esta Institución en lo que contradigan o se opongan a lo dispuesto en el presente Acuerdo.

Sevilla, 8 de mayo de 2018.- El Presidente, Antonio M. López Hernández.

00136118