3. Otras disposiciones

CÁMARA DE CUENTAS DE ANDALUCÍA

Resolución de 13 de febrero de 2024, de la Presidenta de la Cámara de Cuentas de Andalucía, por la que se da publicidad al Acuerdo de 9 de noviembre de 2023, del Pleno de la Cámara de Cuentas de Andalucía, por el que se aprueban las normas que regulan la política de seguridad de la información en la Cámara de Cuentas de Andalucía.

La Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, en su artículo 3.2, dispone la obligación de las Administraciones Públicas de relacionarse entre sí a través de medios electrónicos, que aseguren la interoperabilidad y seguridad de los sistemas y soluciones adoptadas por cada una de ellas, así como la de garantizar la protección de los datos de carácter personal. Por otra parte, en su artículo 156, se establece que el Esquema Nacional de Seguridad tiene por objeto establecer la política de seguridad en la utilización de medios electrónicos en el ámbito de dicha norma, estando constituido por los principios básicos y requisitos mínimos que garanticen adecuadamente la seguridad de la información tratada. Esta última disposición ha sido desarrollada a través del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (en adelante, ENS), que ha venido a derogar el Real Decreto 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.

El artículo 12.2 del Real Decreto 311/2022, de 3 de mayo, 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.

No cabe duda del carácter público de las funciones estatutariamente encomendadas a la Cámara de Cuentas de Andalucía y del desarrollo, también, de actividades de contenido puramente administrativo, que aconsejan adoptar una Política de Seguridad de la Información aun cuando este órgano técnico, dependiente del Parlamento de Andalucía, formalmente no aparezca incluido dentro del ámbito subjetivo de aplicación de la Ley 40/2015. A mayor abundamiento, la disposición adicional primera de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, encomienda a los órganos constitucionales o con relevancia constitucional y a las instituciones de las comunidades autónomas análogas a los mismos que apliquen a los tratamientos de datos personales las medidas de seguridad que correspondan de las previstas en el Esquema Nacional de Seguridad. Esa misma disposición también prescribe la implantación de las medidas de seguridad del ENS a las entidades del sector público y a las del sector privado que colaboren con estas en la prestación de servicios públicos que involucren el tratamiento de datos personales. Debe recordarse, por tanto, que la Política de Seguridad de la Información es la primera medida de seguridad a aplicar cualquiera que sea la categoría del sistema de información y la naturaleza de los datos que se traten.

Según el mencionado Real Decreto 311/2022, de 3 de mayo, el ENS está constituido por los principios básicos y requisitos mínimos necesarios para una protección adecuada de la información tratada y los servicios prestados por las entidades de su ámbito de aplicación, con objeto de asegurar el acceso, la confidencialidad, la integridad, la trazabilidad, la autenticidad, la disponibilidad y la conservación de los datos, la información y los servicios utilizados por medios electrónicos que gestionen en el ejercicio de sus competencias.

Como consecuencia, la presente Política de Seguridad de la Información, se puede definir como el conjunto de directrices que rigen la forma en que la Cámara de Cuentas de Andalucía gestiona y protege la información que trata en el ámbito de las competencias

00297181

que le son propias, y será desarrollada a través de las diferentes normativas, guías y procedimientos que se aprueben con la finalidad de que los riesgos sean tratados adecuadamente.

La política de seguridad de la Cámara de Cuentas de Andalucía se ha regido hasta el momento por el Acuerdo del 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. Sin embargo, desde esa fecha se han sucedido determinados cambios normativos, entre los que destacan la aprobación de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos de Carácter Personal y Garantia de Derechos Digitales, y la del mencionado Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

Lo anterior, aconseja la aprobación de una nueva política de seguridad para acomodarla a los estándares de protección de la información y de los datos que resultan exigibles a cualquier Administración Pública. Así, la presente Política de Seguridad de la Información tiene en cuenta los principios básicos que permiten garantizar el cumplimiento de la legislación en materia de protección de datos vigente, acorde con 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 (en adelante RGPD), y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos de Carácter Personal y Garantía de Derechos Digitales. Para su elaboración se han tenido en cuenta, además de la normativa ya citada, las recomendaciones y guías CCN-STIC del Centro Criptológico Nacional, particularmente de la serie 800, relacionadas con el Esquema Nacional de Seguridad.

Por lo expuesto, el Pleno de la Cámara de Cuentas, en el ejercicio legítimo de sus competencias normativas, establecidas en el artículo 19 en relación con el artículo 3.1 de la Ley 1/1988, de 17 de marzo, de la Cámara de Cuentas de Andalucía, y el artículo 10.a) de su Reglamento de Organización y Funcionamiento, ha aprobado en sesión celebrada el día 9 de noviembre de 2023 las siguientes

NORMAS QUE REGULAN LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN EN LA CÁMARA DE CUENTAS DE ANDALUCÍA

Artículo 1. Misión estatutaria y objeto del presente acuerdo.

1. La Cámara de Cuentas de Andalucía es el órgano técnico dependiente del Parlamento de Andalucía al que, sin perjuicio de las competencias que la Constitución atribuye al Tribunal de Cuentas, corresponde la fiscalización externa de la gestión económica, financiera y contable de los fondos públicos de la Comunidad Autónoma de Andalucía.

2. Para la mejor protección de la información que trata en el ejercicio de sus funciones estatutariamente reconocidas, se acuerda aprobar la presente Política de Seguridad de la Información (en adelante PSI) en la Cámara de Cuentas de Andalucía, así como la estructura organizativa necesaria para definirla, implantarla y gestionarla.

Artículo 2. Ámbito de aplicación.

1. La PSI en la Cámara de Cuentas de Andalucía afectará a la información tratada por medios electrónicos y a la información en soporte no electrónico que haya sido causa o consecuencia directa de la información electrónica, gestionada por la Cámara de Cuentas de Andalucía en el ámbito de sus competencias.

2. La PSI y su normativa de desarrollo 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, adscripción o relación con la misma.

00297181

Artículo 3. Marco normativo.

El marco normativo de las actividades de la Cámara de Cuentas de Andalucía, en el ámbito de esta PSI, está integrado por las siguientes normas:

a) Ley Orgánica 2/2007, de 19 de marzo, de reforma del Estatuto de Autonomía para Andalucía.

b) Ley 1/1988, de 17 de marzo, de la Cámara de Cuentas de Andalucía.

c) Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

d) Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

e) Real Decreto Legislativo 5/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto Básico del Empleado Público.

f) Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014.

g) Ley 7/2011, de 3 de noviembre, de Documentos, Archivos y Patrimonio Documental de Andalucía.

h) 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 y por el que se deroga la Directiva 95/46/CE (RGPD).

i) Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales.

j) Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.

k) Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

l) Reglamento de Organización y Funcionamiento, aprobado por la Comisión de Hacienda y Administración Pública del Parlamento de Andalucía, en sesión celebrada el 21 de diciembre de 2011.

m) Acuerdo de 24 de enero de 2022, de la Cámara de Cuentas de Andalucía, por el que se regula la creación de la sede electrónica de la Cámara de Cuentas de Andalucía.

n) Acuerdo de 10 de febrero de 2022, de la Cámara de Cuentas de Andalucía, por el que se regula la creación y funcionamiento del registro electrónico de la Cámara de Cuentas de Andalucía.

o) Acuerdo de 10 de marzo de 2022, de la Cámara de Cuentas de Andalucía, por el que se establece la obligación de cualquier persona física de relacionarse con esta institución a través de medios electrónicos para determinados procedimientos, y la obligación para el personal a su servicio para los trámites y actuaciones que realicen por razón de su condición de empleado público.

p) Aquellas normas aplicables a la administración electrónica y a la seguridad de la información que complementen, desarrollen o sustituyan a las anteriores y que se encuentren dentro del ámbito de aplicación de la Política de Seguridad de la Información de la Cámara de Cuentas de Andalucía.

Artículo 4. Principios de la seguridad de la información.

1. Principios básicos. 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. Complementando lo dispuesto en el capítulo II del Real Decreto 311/2022, de 3 de mayo, se establecen los siguientes principios básicos:

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.

00297181

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 de desarrollar la forma concreta de implementar la seguridad en el sistema y de la supervisión de la operación diaria del mismo, pudiendo delegar en administradores u operadores bajo su responsabilidad; y el responsable de la seguridad, que será distinto del responsable del sistema, que determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios, supervisará la implantación de las medidas necesarias para garantizar que se satisfacen los requisitos y reportará sobre estas cuestiones. En los supuestos de tratamientos de datos personales se identificará además a la persona o unidad responsable del tratamiento y, en su caso, al encargado de tratamiento, de acuerdo con las definiciones del artículo 4, apartados 7 y 8, del RGPD.

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 de información, evitando, salvo casos de urgencia o necesidad, cualquier actuación puntual o tratamiento coyuntural. 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 los Riesgos: El análisis y gestión de riesgos será parte esencial del proceso de seguridad. La gestión de los riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. La reducción a estos niveles se realizará mediante el despliegue de medidas de seguridad, que establecerán 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. Además, las medidas de seguridad deberán garantizar el cumplimiento de lo previsto en el artículo 32 del RGPD, por lo que el responsable del tratamiento de datos personales, y en su caso, los encargados del tratamiento, podrán adoptar todas aquellas medidas adicionales con el fin de garantizar la seguridad de los datos personales, en virtud de lo dispuesto en los artículos 24 y 25 del RGPD, en el artículo 28 de la Ley Orgánica 3/2018, de 5 de diciembre, y en el artículo 3 del Real Decreto 311/2022, de 3 de mayo.

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 a la constante evolución de los riesgos y sistemas de protección. La seguridad de la información será atendida, revisada y auditada por personal cualificado, instruido y con dichas competencias entre sus funciones.

g) Seguridad desde el diseño y por defecto: Los sistemas deben diseñarse y configurarse de forma que garanticen un grado suficiente de seguridad por defecto. Además, con el fin de garantizar la resiliencia y la protección de los datos personales, se deben tener en cuenta las medidas de seguridad por defecto en base a los artículos 24 y 25 del RGPD, así como las medidas de seguridad orientadas al riesgo según el artículo 32 del RGPD.

h) Vigilancia continua: De forma que la evaluación permanente del estado de la seguridad de los activos permita medir su evolución, detectando vulnerabilidades e identificando deficiencias de configuración. En cuanto la gestión de incidentes que afecten a datos personales, se tendrá en cuenta las obligaciones específicas de notificación, comunicación y documentación especificadas en los artículos 33 y 34 del RGPD.

i) Prevención, detección, respuesta y conservación: Se deben aplicar estos principios, de manera que las amenazas existentes no se materialicen o, en el caso de materializarse, no afecten gravemente a la información que se trata o a los servicios prestados.

00297181

Prevención: Para prevenir en la medida de lo posible que la información o los servicios se vean afectados por incidentes de ciberseguridad, deberán implantarse las medidas mínimas de seguridad determinadas por el ENS, así como cualquier control identificado a través de una evaluación de amenazas y riesgos.

Detección: Se deberá monitorizar la operativa de manera continua para detectar anomalías en los niveles de prestación de los servicios y poder actuar en consecuencia. Se establecerán mecanismos de detección, análisis y reporte que lleguen a las personas responsables de forma periódica y cuando se produzca una desviación significativa de los parámetros que se hayan establecido como normales.

Respuesta: Para cumplir con este principio se deberán:

i) Establecer mecanismos para responder eficazmente a los incidentes de seguridad.

ii) Designar puntos de contacto para las comunicaciones con respecto a incidentes detectados en los distintos departamentos.

iii) Establecer protocolos para el intercambio de información relacionada con el incidente. Esto incluye comunicaciones, en ambos sentidos, con los Equipos de Respuesta a Emergencias (CERT).

Conservación: Para cumplir con este principio y para garantizar la disponibilidad de los servicios críticos, se deberán desarrollar planes de continuidad de los sistemas TIC y actividades de recuperación.

2. Principios particulares y responsabilidades específicas. Las directrices fundamentales de seguridad se concretan en un conjunto de principios particulares y responsabilidades específicas, que se configuran como objetivos instrumentales que garantizan el cumplimiento de los principios básicos de la PSI y que inspiran las actuaciones de la Cámara de Cuentas en dicha materia. Se establecen los siguientes principios particulares y responsabilidades específicas:

a) Protección de datos de carácter personal: se adoptarán las medidas técnicas y organizativas destinadas a garantizar el nivel de seguridad exigido por la normativa vigente en relación con el tratamiento de los datos de carácter personal.

b) Gestión de activos de información: Los activos de información de la Cámara de Cuentas se encontrarán inventariados y categorizados y estarán 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 activos de información serán emplazados en áreas 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 o ambientales.

e) Seguridad en la gestión de 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 se transmita a través de redes de comunicaciones deberá ser adecuadamente protegida, teniendo en cuenta su nivel de sensibilidad y de criticidad, mediante mecanismos que garanticen su seguridad. Para proteger las redes de la Cámara de Cuentas, se analizará el tráfico cifrado de usuarios de forma automatizada. Se realizará la excepción en este análisis de las categorías de navegación relacionadas con datos sensibles especialmente protegidos de acuerdo con la normativa de protección de datos vigente, siempre que sea posible la discriminación.

f) Control de acceso: Se limitará el acceso a los activos de información por parte de usuarios, procesos y otros sistemas de información mediante la implantación de los mecanismos de identificación, autenticación y autorización acordes a la criticidad de cada activo. Además, quedará registrada la utilización del sistema con objeto de asegurar

00297181

la trazabilidad del acceso y auditar su uso adecuado, conforme a la actividad de la organización.

g) Adquisición, desarrollo y mantenimiento de los sistemas de información: Se contemplarán los aspectos de seguridad de la información en todas las fases del ciclo de vida de los sistemas de información, garantizando su seguridad por defecto.

h) Gestión de los incidentes de seguridad: 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 con 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.

3. Sin perjuicio de lo establecido en los apartados 1 y 2, la presente PSI se establecerá en base a los principios básicos contemplados en el capítulo II del Real Decreto 311/2022, de 3 de mayo, y se desarrollará aplicando los requisitos mínimos contemplados en el artículo 12.6 de la misma disposición reglamentaria.

Artículo 5. Estructura organizativa.

1. La estructura organizativa para la gestión de la seguridad de la información en la Cámara de Cuentas de Andalucía, de acuerdo con el principio de función diferenciada, estará compuesta por los siguientes agentes:

a) Comité de Dirección de Seguridad de la Información.
b) Responsable de Seguridad.
c) Responsable del Sistema de Información.
d) Responsables de la Información y de los Servicios.
e) Delegado de Protección de Datos.

2. Las funciones atribuidas a los distintos agentes responsables de la gestión de la seguridad de la información habrán de ser interpretadas sin perjuicio de las atribuciones de los distintos órganos de la Cámara de Cuentas de Andalucía previstas en la Ley 1/1988, de 17 de marzo, y en su Reglamento de Organización y Funcionamiento.

Artículo 6. Comité de Dirección de Seguridad de la Información.

1. Se crea, adscrito a la Presidencia de la Cámara de Cuentas de Andalucía, el Comité de Dirección de Seguridad de la Información (en adelante, CDSI), como órgano colegiado de los previstos en el artículo 22.2 de la Ley 40/2015, de 1 de octubre, que gestionará y coordinará todas las actividades relacionadas con la seguridad de los sistemas de información.

2. El CDSI estará compuesto por los siguientes miembros:

a) Presidencia: La persona titular de la Presidencia de la Cámara de Cuentas de Andalucía.

b) Vocales:

i) La persona titular de la Secretaría General de la Cámara de Cuentas de Andalucía.
ii) La persona titular de la Coordinación de la Secretaría General y de la Jefatura del Gabinete Jurídico.
iii) La persona titular de la Coordinación del Departamento de Coordinación.
iv) La persona titular de la Jefatura del Servicio de Tecnologías de la Información.
v) Delegado de Protección de Datos.
vi) Responsable de Seguridad, quien actuará como secretario

3. El régimen de suplencia de la presidencia y secretaría, en caso de vacante, ausencia o enfermedad, así como en los casos en que haya sido declarada su abstención

00297181

o recusación y, en general, cuando concurra alguna causa justificada, se establece del siguiente modo:

i) La persona titular de la Presidencia será sustituida por la persona titular de la Vicepresidencia de la Cámara de Cuentas de Andalucía.

ii) El secretario del CDSI podrá ser sustituido por otro funcionario de la Cámara designado por la Presidencia.

4. Adicionalmente, podrán ser invitados a asistir al CDSI los responsables de materias específicas a tratar, en función del contenido del orden del día, que actuarán con voz pero sin voto.

5. El CDSI ejercerá las siguientes funciones:

a) Impulsar el desarrollo normativo de la PSI y velar por el cumplimiento de la PSI y demás normativa de seguridad aprobada por el Pleno.

b) Promover revisiones y actualizaciones de la PSI y de su normativa de desarrollo.

c) Proporcionar soporte, asesoramiento e información al Pleno de la Cámara de Cuentas de Andalucía, así como ejecutar los acuerdos adoptados por éste en materia de seguridad de la información.

d) Aprobación de guías de seguridad a propuesta del responsable de seguridad.

e) Resolver los conflictos que puedan surgir entre los diferentes agentes participantes en la gestión de la seguridad de la información.

f) Ordenar la realización de las auditorías o autoevaluaciones de seguridad y recibir información de los resultados de las mismas. En este sentido, también podrá definir la planificación de estas actuaciones, que en todo caso deberán ser regulares.

g) Aprobar los planes de mejora de la seguridad en su ámbito de competencias.

h) Tomar conocimiento de las decisiones y medidas tomadas para satisfacer los requisitos de seguridad de la información y de los servicios.

i) Establecer los requisitos de seguridad que deben cumplir, a nivel organizativo, técnicos y de control, los sistemas y servicios de la Cámara de Cuentas de Andalucía.

j) Tomar conocimiento de los incidentes de seguridad que se produzcan.

k) Promover la formación y concienciación en materia de seguridad de la información a todo el personal, definiendo los programas formativos y de concienciación relacionados con buenas prácticas de seguridad TIC en el ámbito de la Cámara de Cuentas de Andalucía.

l) Aprobación y revisión anual del Proceso de Gestión de Riesgos especificado en el artículo 11.

6. Las sesiones del CDSI se considerarán debidamente constituidas, cuando asistan a sus reuniones al menos la persona titular de la presidencia y el secretario del CDSI, o personas que las sustituyan, y otros dos vocales.

7. El CDSI se reunirá con carácter ordinario al menos una vez al año, y con carácter extraordinario cuando lo decida la persona titular de la Presidencia.

8. El CDSI se regirá por las normas de funcionamiento previstas en el presente acuerdo y, en lo no contemplado en ellas, por las normas previstas para los órganos colegiados en la Sección 3.ª del Capítulo II del Título Preliminar de la Ley 40/2015, de 1 de octubre.

Artículo 7. Responsable de Seguridad.

1. En base a lo dispuesto en el artículo 13.2.c) del Real Decreto 311/2022, de 3 de mayo, el responsable de la seguridad determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios, supervisará la implantación de las medidas necesarias para garantizar que se satisfacen los requisitos y reportará sobre estas cuestiones.

2. Serán funciones de la persona Responsable de Seguridad:

a) Supervisar el cumplimiento de la PSI y su normativa de desarrollo, así como de las guías y procedimientos de seguridad que se aprueben.

00297181

b) Impulsar en el seno del CDSI, la aprobación, revisión y actualización de la PSI y su normativa de desarrollo, así como de las guías de seguridad aprobadas por el CDSI.

c) Elaborar, con la colaboración de la persona Responsable del Sistema de Información, procedimientos de seguridad orientados a resolver las tareas, consideradas críticas por el perjuicio que causaría una actuación inadecuada, de seguridad, desarrollo, mantenimiento y explotación de los sistemas de información.

d) Mantener ordenada y actualizada la documentación, aprobada o elaborada en el ámbito de la seguridad de la información, gestionando los mecanismos de acceso a la misma.

e) Coordinar la interacción con organismos y entidades especializadas en el ámbito de la seguridad de la información, compartiendo experiencias y conocimiento que ayuden a mejorar y mantener la seguridad de los sistemas de la Cámara de Cuentas de Andalucía.

f) Monitorización de los incidentes de seguridad y supervisar su investigación.

g) Habilitar y mantener un registro de incidencias para la seguridad de la información que esté bajo su responsabilidad. Este registro deberá estar disponible para cualquier revisión o auditoría.

h) Analizar los informes de autoevaluación y auditoría de la seguridad de la información.

i) Realizar análisis de riesgos en tiempo y forma, contando con la colaboración de los correspondientes Responsables de la Información y de los Servicios.

j) Identificar las categorías de seguridad de los sistemas de información y determinar, de entre las medidas de seguridad indicadas en el Anexo II del Real Decreto 311/2022, las más adecuadas y eficaces para satisfacer los requisitos de seguridad de la información y de los servicios, sin perjuicio de la necesaria autorización por el Secretario General de la Cámara de Cuentas para la efectiva implementación de aquéllas. Las medidas de seguridad previstas en el Anexo II del Real Decreto 311/2022 podrán ser ampliadas o reemplazadas por otras compensatorias, de conformidad con el artículo 28 del referido real decreto.

k) Firmar la Declaración de Aplicabilidad de las medidas de seguridad seleccionadas.

l) Supervisar la implantación de las medidas de seguridad.

m) Obtener las certificaciones exigibles a la figura de los Responsables de la Seguridad, en base a lo dispuesto en el artículo 13.4 del Real Decreto 311/2022, de 3 de mayo.

n) Mantener un listado actualizado del personal autorizado a acceder a los sistemas de información.

o) Autorizar los permisos de acceso a los usuarios sobre los recursos, (automatizados y no automatizados) que se encuentran bajo su responsabilidad y que sean estrictamente necesarios para el desarrollo de las funciones del trabajador.

p) Revisar los permisos y perfiles de acceso de la información que se encuentran bajo su gestión.

q) Promover y ejecutar actividades de concienciación y formación en materia de seguridad en su ámbito de responsabilidad, siguiendo las directrices del CDSI.

3. En su condición de secretario del CDSI, la persona Responsable de seguridad tiene como funciones:

a) Efectuar la convocatoria de las reuniones del CDSI.

b) Preparar los temas a tratar en las reuniones del CDSI, aportando información puntual para la toma de decisiones, preparando todos los trabajos previos necesarios para las reuniones, apoyándose cuando lo requiera en las distintas unidades y departamentos de la Cámara de Cuentas de Andalucía.

c) Elaborar el acta de las reuniones.

d) Velar por la ejecución de las decisiones del CDSI.

4. El rol de Responsable de seguridad será desempeñado por el funcionario o funcionaria de carrera que designe la persona titular de la Presidencia de la Cámara de

00297181

Cuentas de Andalucía, que en todo caso será distinto de la persona Responsable del Sistema de Información. Sin perjuicio de su dependencia orgánica, reportará directamente a la persona titular de la Presidencia de la Cámara de Cuentas, a la persona titular de la Secretaría General y al CDSI en relación con sus funciones como Responsable de Seguridad.

Artículo 8. Responsable del Sistema de Información.

1. De acuerdo con lo previsto en el artículo 13.2.d) del Real Decreto 311/2022, de 3 de mayo, la persona Responsable del Sistema de Información se encargará de desarrollar la forma concreta de implementar la seguridad en el sistema y de la supervisión de la operación diaria del mismo, pudiendo delegar en administradores u operadores bajo su responsabilidad.

2. Dentro de sus funciones se encuentran las siguientes:

a) Definir la tipología y sistemas de gestión de los sistemas de información, estableciendo los criterios de uso y los servicios disponibles en éstos.

b) Cerciorarse de que las medidas de seguridad se integran adecuadamente dentro del marco tecnológico y de seguridad de la Cámara de Cuentas.

c) Adoptar las medidas correctoras adecuadas de acuerdo con las evaluaciones y auditorías de seguridad.

d) Responsabilizarse del desarrollo, operación y mantenimiento de los sistemas de información durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.

e) Aprobar toda modificación sustancial de la configuración de cualquier elemento del sistema.

f) Colaborar con el Responsable de Seguridad en la elaboración de procedimientos de seguridad de los sistemas de información.

g) Elaborar planes de continuidad de los sistemas de información.

h) Acordar la suspensión del manejo de determinada información o la prestación de un cierto servicio si es informado de deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos. Esta decisión deberá ser acordada con las personas Responsables de la Información y Servicios afectadas, y la persona Responsable de Seguridad antes de ser ejecutada, e informado el CDSI.

3. El rol de Responsable del Sistema de Información recaerá en la persona titular de la Jefatura del Servicio de Tecnologías de la Información.

Artículo 9. Responsables de la Información y de los Servicios.

1. De acuerdo con lo dispuesto en el artículo 13.2.a) y b) del Real Decreto 311/2022, de 3 de mayo, las personas Responsables de la Información y de los Servicios serán quienes, dentro de la organización, decidan los requisitos de la información tratada y de los servicios prestados, siendo los responsables últimos de su uso y acceso y, por lo tanto, de su mantenimiento y protección. Las principales funciones, dentro de su ámbito de actuación, serán las siguientes:

a) Determinar los requisitos de seguridad de la información que se maneja y de los servicios que presta, clasificando la información tratada o los servicios prestados conforme a los criterios y categorías establecidas en el ENS y en cada una de las dimensiones de seguridad conocidas y aplicables (Disponibilidad, Autenticidad, Trazabilidad, Confidencialidad e Integridad), dentro del marco establecido en el Anexo I del ENS.

b) Solicitar a la persona Responsable de Seguridad el preceptivo análisis de riesgos y proporcionarle la información necesaria. Para ello, contarán con la ayuda de la persona Responsable del Sistema de Información.

c) Verificar que los análisis de riesgos realizados se corresponden en todo momento con la información aportada para la realización de los mismos.

00297181

d) Aceptar los riesgos residuales calculados en el análisis de riesgos y realizar su seguimiento y control, sin perjuicio de la posibilidad de delegar esta última tarea.

e) Impulsar la ejecución de auditorías de seguridad.

2. A los efectos previstos en el RGPD, las personas Responsables de la Información y de los Servicios determinan los fines y medios del correspondiente tratamiento de datos personales. En consecuencia, la Cámara de Cuentas ostenta la consideración de responsable del tratamiento respecto de los datos personales contenidos en la información incluida en su ámbito de actuación.

3. Las personas Responsables de la Información y de los Servicios serán designadas por la persona titular de la Presidencia de la Cámara de Cuentas.

Artículo 10. Delegado de Protección de Datos.

1. El Delegado de Protección de Datos tiene carácter asesor y supervisor para el cumplimiento de lo dispuesto en el RGPD, en la Ley Orgánica 3/2018, de 5 de diciembre, y demás normativa aplicable sobre protección de datos personales.

2. Sin perjuicio de las funciones que le atribuye el RGPD, en el ámbito de la presente norma, el asesoramiento y supervisión del Delegado de Protección de Datos se extiende a aquellas medidas de seguridad que se quieran implementar con finalidades distintas a garantizar la protección de datos, en la medida que impliquen un tratamiento adicional de datos personales.

3. Dentro de la gestión general de incidentes, el Delegado de Protección de Datos intervendrá en la gestión de las brechas de datos personales, principalmente en su posición de interlocutor de Cámara de Cuentas ante la Agencia Española de Protección de Datos o el Consejo de Transparencia y Protección de Datos de Andalucía.

Artículo 11. Gestión de los Riesgos.

1. La gestión de riesgos debe realizarse de manera continua sobre los sistemas de información, conforme a los principios de gestión de la seguridad basada en los riesgos, vigilancia continua y reevaluación periódica, previstos en los artículos 7 y 10 del Real Decreto 311/2022, de 3 de mayo.

2. El Proceso de Gestión de Riesgos, que comprende la definición de 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, deberá revisarse y aprobarse cada año por el CDSI. El Proceso de Gestión de Riesgos aprobado conformará la guía metodológica básica para la elaboración de los respectivos análisis de riesgos, y por lo tanto facilitará la homogenización y comparación de los resultados de cada uno de los análisis de riesgos que se realicen.

3. Las indicadas fases del proceso de gestión de riesgos se realizarán según lo dispuesto en los anexos I y II del Real Decreto 311/2022, de 3 de mayo, y siguiendo las normas, instrucciones, guías CCN-STIC y recomendaciones para la aplicación del mismo elaboradas por el Centro Criptológico Nacional.

4. Las personas Responsables de la Información y de los Servicios solicitarán al Responsable de la Seguridad el preceptivo análisis de riesgos para que se proponga el tratamiento adecuado, calculando los riesgos residuales, identificando carencias y debilidades.

5. Se realizará un análisis de riesgos:

a) Regularmente, una vez al año.

b) Cuando haya cambios en los servicios esenciales prestados o cambios significativos en las infraestructuras que los soportan.

c) Cuando ocurra un incidente de seguridad grave.

d) Cuando se identifiquen amenazas severas que no hubieran sido tenidas en cuenta o vulnerabilidades graves que no estén contrarrestadas por las medidas de protección implantadas.

00297181

6. La persona Responsable de la Seguridad será la encargada de realizar el análisis de riesgos en tiempo y forma, contando con la colaboración de los correspondientes Responsables de la Información y de los Servicios.

7. Tras la calificación de la información y la determinación de la categoría de seguridad del sistema, se obtendrá la matriz de aplicabilidad y el conjunto de medidas para garantizar la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información y del servicio. La evaluación de los riesgos se realizará identificando los riesgos residuales.

8. Será responsabilidad de los Responsables de la Información y de los Servicios, la aceptación de los riesgos residuales y el impulso de la ejecución de auditorías de seguridad.

9. En el caso de que existan tratamientos de datos personales, se deberá tener en cuenta lo dispuesto en el artículo siguiente, de modo que los requisitos identificados conforme a dicho artículo y, con el asesoramiento específico del Delegado de Protección de Datos, se puedan añadir a los establecidos conforme al Real Decreto 311/2022, de 3 de mayo, si así fuera necesario, en particular, fijando el nivel de seguridad a un nivel más alto. En estos casos, si el resultado del análisis es que los tratamientos de datos personales fuesen de alto riesgo, estos requisitos se elaborarán con la formalidad de una evaluación de impacto en la protección de datos, conforme al artículo 35 del RGPD y los criterios establecidos por la Agencia Española de Protección de Datos (AEPD). En este aspecto también se deberá tener en cuenta la regulación de la seguridad de los tratamientos de datos personales, especificada en el artículo 32 del RGPD.

Artículo 12. Protección de datos de carácter personal.

1. Se aplicarán a los datos de carácter personal que sean objeto de tratamiento por parte de la Cámara de Cuentas de Andalucía, las medidas de seguridad apropiadas derivadas del análisis de riesgos, así como de la evaluación de impacto relativa a la protección de datos, que se detalla en el RGPD y en la Ley Orgánica 3/2018, de 5 de diciembre.

2. Además, se aplicarán las medidas correspondientes al Anexo II del Real Decreto 311/2022, de 3 de mayo. En el caso de que el análisis de riesgos determine medidas agravadas respecto a la normativa recogida en las medidas del citado Anexo, las medidas derivadas del análisis de riesgos serán las que se implementarán en la protección de datos de carácter personal.

3. En particular, se tendrá en cuenta el artículo 32 del RGPD, en cuanto a la exigencia de una identificación de riesgos específicos para los derechos y libertades de las personas en relación a los tratamientos de datos personales, que debe ser previo al análisis de riesgos de los sistemas donde se implementen dichos tratamientos, de forma que la categoría de seguridad sea adecuada al riesgo que los tratamientos de datos personales suponen para los derechos y libertades de las personas.

4. El Responsable del Sistema de Información o los administradores u operadores en los que delegue, podrán implementar tratamientos de datos personales como consecuencia de la implantación de medidas de seguridad que tengan un objeto distinto que la protección de los datos personales, en base a lo dispuesto en el artículo 24 del Real Decreto 311/2022, de 3 de mayo, y teniendo en cuenta, entre otros, los principios de limitación de finalidad; prohibición del tratamiento de los datos personales para fines distintos; el principio de minimización de datos, identificando los datos personales o las categorías de datos personales que pudieran ser tratados; o del principio de limitación del plazo de conservación, identificando los plazos máximos de conservación de los datos personales.

Artículo 13. Niveles de desarrollo.

1. La PSI de la Cámara de Cuentas será desarrollada a través de las diferentes normativas, guías y procedimientos que se aprueben, con la finalidad de que los riesgos sean tratados adecuadamente.

00297181

2. La documentación relativa a la seguridad de la información estará clasificada en cuatro niveles, de manera que los documentos de nivel inferior estén siempre alineados con los de nivel superior:

a) Primer nivel: PSI y normativa de desarrollo.

Documentos de obligado cumplimiento para todo el personal, interno y externo de la Cámara de Cuentas de Andalucía.

La normativa de desarrollo debe estar alineada con la PSI y, al igual que ésta, debe ser aprobada por acuerdo del Pleno de la Cámara de Cuentas.

b) Segundo nivel: Guías de seguridad.

Documentos de carácter eminentemente formativo que tienen por objeto ayudar a los usuarios a aplicar correctamente las medidas de seguridad adoptadas, proporcionando razonamientos donde no existen procedimientos precisos.

La responsabilidad de la aprobación de los documentos redactados en este nivel será competencia del Comité de Dirección de Seguridad de la Información, a propuesta de la persona Responsable de Seguridad.

c) Tercer nivel: Procedimientos de seguridad.

Documentos orientados a resolver las tareas, consideradas críticas por el perjuicio que causaría una actuación inadecuada, de seguridad, desarrollo, mantenimiento y explotación de los sistemas de información.

Corresponde elaborar estos procedimientos a la persona Responsable de Seguridad, con la colaboración de la persona Responsable del Sistema de Información.

d) Cuarto nivel: Informes, registros y evidencias electrónicas. Se definen, respectivamente, como:

i) Documentos de carácter técnico que recogen el resultado y las conclusiones de un estudio o una valoración.

ii) Documentos de carácter técnico que recogen amenazas y vulnerabilidades de los sistemas de información.

iii) Evidencias electrónicas generadas durante todas las fases del ciclo de vida del sistema de información.

3. En la elaboración de la normativa, guías y procedimientos en materia de seguridad de la información, se tendrán en cuenta:

a) Las guías de seguridad de las tecnologías de la información y la comunicación elaboradas por el Centro Criptológico Nacional (guías CCN-STIC).

b) Las normas o recomendaciones aprobadas por órganos y organismos con competencias en materia de seguridad o de protección de datos, como son el Centro Criptológico Nacional, la Agencia Española de Protección de Datos, el Centro de Seguridad TIC de Andalucía (Andalucía-CERT) o el Consejo de Transparencia y Protección de Datos de Andalucía.

c) Las recomendaciones, guías de configuración y buenas prácticas publicadas por organismos u organizaciones internacionales y por los fabricantes de productos de seguridad.

Artículo 14. Obligaciones del personal.

1. Todos los miembros de la Cámara de Cuentas, así como el personal a su servicio, tienen la obligación de conocer y cumplir la presente PSI y su normativa de desarrollo, así como las guías y procedimientos de seguridad aplicables a su ámbito de actuación, siendo responsabilidad del CDSI disponer los medios necesarios para que la información llegue a todos los afectados. Igualmente, esta obligación se aplicará a las personas que ocasionalmente presten servicios a la Cámara de Cuentas de Andalucía mediante una relación contractual sometida a la legislación de contratos públicos.

2. El incumplimiento manifiesto de la PSI o su normativa de desarrollo, así como de los protocolos y procedimientos de seguridad aprobados, podrá acarrear, en su caso, las responsabilidades disciplinarias que correspondan.

00297181

Artículo 15. Concienciación y formación.

1. Todo el personal relacionado con la información, los servicios y los sistemas de información, deberá ser formado e informado de sus deberes y obligaciones en materia de seguridad de la información.

2. Para garantizar la seguridad de las tecnologías de la información aplicables a los sistemas y servicios de la Cámara de Cuentas de Andalucía, se articularán los mecanismos necesarios para llevar a la práctica la concienciación y la formación específica necesaria e imprescindible en todos los niveles de la organización.

Artículo 16. Terceros.

1. Cuando se presten servicios o se gestione información de otras organizaciones, se les hará participe de esta política de seguridad de la información, se establecerán canales para reporte y coordinación de los respectivos comités de seguridad de la Información y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

2. Cuando se utilicen servicios de terceros o ceda información a terceros, se les hará participes de esta política de seguridad y de la normativa de seguridad que ataña a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de reporte y resolución de incidencias.

3. Se garantizará que el personal de terceros está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta política.

4. Cuando algún aspecto de la PSI no pueda ser satisfecho por una tercera parte según se requiere en los apartados anteriores, se requerirá un informe del Responsable de Seguridad que precise los riesgos en que se incurre y la forma de tratarlos. Ese riesgo deberá ser aceptado por el CDSI.

5. Las terceras partes involucradas en tratamientos de datos de carácter personal deberán satisfacer los requisitos establecidos por la Cámara de Cuentas de Andalucía y deberán formalizar su relación como encargados de tratamientos.

Disposición adicional. Actualización permanente de la Política de Seguridad de la Información.

La PSI de la Cámara de Cuentas deberá mantenerse actualizada permanentemente para adecuarla a la evolución tecnológica y al desarrollo de la sociedad de la información, así como a los estándares internacionales de seguridad.

Disposición derogatoria.

Queda derogado el Acuerdo del 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, así como cuantas disposiciones de esta Institución se opongan a lo dispuesto en el presente acuerdo.

Disposición final.

El presente acuerdo será publicado en el Boletin Oficial de la Junta de Andalucía y entrará en vigor el día siguiente al de su publicación.

Sevilla, 13 de febrero de 2024.- La Presidenta, Carmen Núñez García.

00297181