RESOLUCIÓN DE LA DIRECCIÓN DE LA AGENCIA PARA LA CALIDAD CIENTÍFICA Y UNIVERSITARIA DE ANDALUCÍA (ACCUA) POR LA QUE SE APRUEBA LA POLÍTICA DE SEGURIDAD INTERIOR, TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES, Y PROTECCIÓN DE DATOS PERSONALES DE ACCUA

ANTECEDENTES

La Administración de la Junta de Andalucía mediante el Decreto 1/2011, de 11 de enero, modificado por el Decreto 70/2017, de 6 de junio, aprobó la Política de Seguridad de las Tecnologías de la Información y Comunicaciones en la Administración de la Junta de Andalucía, disponiendo que las distintas Consejerías y demás entidades deberán disponer formalmente de sus propias normas específicas de política de seguridad TIC, y adecuar, en su caso, las directrices comunes de la Administración de la Junta de Andalucía a sus particularidades.

Asimismo, cada Consejería y entidad deberá contar con un Comité de Seguridad de las Tecnologías de la Información y Comunicación (en adelante, TIC), que actuará como una unidad administrativa especial de dirección y seguimiento en materia de seguridad y con los demás perfiles previstos en el Real Decreto 311/2022, de 3 de mayo , por el que se regula el Esquema Nacional de Seguridad (en adelante, ENS).

El ENS se encuentra establecido en el artículo 156.2 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, regulado por el Real Decreto 311/2022, de 3 de mayo, y 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. Su finalidad última es la creación de las condiciones necesarias de confianza en el uso de los medios electrónicos, a través de medidas dirigidas a garantizar la seguridad de los sistemas, los datos, las comunicaciones, y los servicios electrónicos, que permitan a la ciudadanía y a las Administraciones Públicas, el ejercicio de derechos y el cumplimiento de deberes a través de estos medios. En este contexto, el ENS exige que todo el sector público cuente con una política de seguridad formalmente aprobada por el órgano competente que ostente las máximas competencias ejecutivas.

Por otro lado, el Decreto 171/2020, de 13 de octubre, por el que se establece la Política de Seguridad Interior en la Administración de la Junta de Andalucía, define un completo sistema de prevención y reacción ante daños en las personas, el patrimonio y el funcionamiento, intencionadamente provocados por agentes externos, personal propio o personas usuarias. Este decreto regula un modelo organizativo funcional en el que por simplificación, eficacia y eficiencia se ha evitado la creación de un Comité de Seguridad Interior, optando por incluir las que hubieran sido sus funciones y tareas entre las de los ya existentes comités de seguridad TIC. En este sentido, en su disposición final primera, modifica el reseñado Decreto 1/2011, de 11

de enero, indicando que “Todas las alusiones en el texto a los «Comités de Seguridad TIC de las entidades» quedan sustituidas por Comités de Seguridad Interior y Seguridad TIC de las Consejerías o entidades dependientes singulares”. Por otra parte, el artículo 10.1 del reseñado Decreto 171/2020, de 13 de octubre, establece que partiendo de sus propios recursos directos, en aquellas entidades dependientes en las que éstas lo consideren necesario por virtud del volumen o singularidad de los activos se contará con una Unidad de Seguridad Interior que ejerza la responsabilidad ejecutiva para la seguridad interior de los activos en su ámbito, debiendo ser designada por el Comité de Seguridad Interior y Seguridad TIC.

Por último, 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 (en adelante, LOPDGDD) determina que los responsables enumerados en el artículo 77.1 de la citada ley, deberán aplicar a los tratamientos de datos personales las medidas de seguridad que correspondan de las previstas en el ENS. Por su parte, la normativa reguladora del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, en su artículo 3 establece que cuando un sistema de información trate datos personales le será de aplicación lo dispuesto en el RGPD y en la LOPDGDD, o en su caso, la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales, el resto de normativa de aplicación, así como los criterios que se establezcan por la Agencia Española de Protección de Datos o en su ámbito competencial, por las autoridades autonómicas de protección de datos.

Por lo tanto, la aplicación de la normativa sobre protección de datos de carácter personal supone para la Agencia para la Calidad Científica y Universitaria de Andalucía (en lo sucesivo, ACCUA), en tanto responsable y también encargada de tratamientos de esta naturaleza, según el caso, que sea necesario la adopción de una serie de medidas de carácter técnico y organizativo tendentes a garantizar los derechos de las personas titulares de dicho datos personales.

En consecuencia, la convergencia de los requisitos de seguridad interior, los referidos requisitos sobre los sistemas de información, y los exigidos para la protección de datos personales hacen aconsejable no acometer acciones desagregadas, que atiendan a cada dimensión por separado, pues ello podría provocar duplicidades, antinomias, confusión y descoordinación internas, además de resultar más oneroso desde el punto de vista de la inversión de recursos humanos, económicos, técnicos y organizativos.

Son de aplicación y sirven de motivación a la presente resolución los siguientes

FUNDAMENTOS DE DERECHO

Primero.- En virtud de lo dispuesto en el artículo 10 del 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, cada Consejería y entidad incluida en el ámbito de aplicación de dicho Decreto deberá disponer formalmente

de su propio documento de política de seguridad TIC, así como de las disposiciones de desarrollo que adecuen, en su caso, las directrices comunes de la Administración de la Junta de Andalucía a sus particularidades. Asimismo, cada Consejería y entidad deberá contar con un Comité de Seguridad TIC, que no tendrá carácter colegiado y que actuará como órgano de dirección y seguimiento en materia de seguridad de los activos TIC de su titularidad o cuya gestión tenga encomendada. El documento de política de seguridad TIC será aprobado por la persona titular de la Consejería o entidad correspondiente.

Segundo.- Según lo dispuesto en el artículo 9 del Decreto 171/2020, de 13 de octubre, por el que se establece la Política de Seguridad Interior en la Administración de la Junta de Andalucía se modifican los Comités a los que alude el artículo 10 del 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 añadiéndoles las funciones de dirección y seguimiento en materia de seguridad interior, cambiando su denominación a "Comités de Seguridad Interior y Seguridad TIC" en virtud de la Disposición final primera de dicho Decreto.

Tercero.- La Ley 9/2021, de 23 de diciembre, por la que se crean la la Agencia Empresarial para la Transformación y el Desarrollo Económico (TRADE) y la Agencia para la Calidad Científica y Universitaria de Andalucía (ACCUA) en su artículo 21 dispone que el funcionamiento efectivo de ACCUA se iniciará el día de la entrada en vigor del decreto del Consejo de Gobierno por el que se aprueben sus estatutos, circunstancia que se produjo el 1 de marzo de 2023, tras la publicación en el Boletin Oficial de la Junta de Andalucía del Decreto 17/2023, de 14 de febrero, por el que se aprueban los Estatutos de la Agencia para la Calidad Científica y Universitaria de Andalucía.

Cuarto.-De conformidad con el artículo 21 del Decreto 17/2023, de 14 de febrero, por el que se aprueban los Estatutos de la Agencia para la Calidad Científica y Universitaria de Andalucía (ACCUA), le corresponden a la Dirección de la Agencia la representación legal ordinaria de la Agencia, sin perjuicio de las competencias de la Presidencia.

Vistos los Antecedentes de Hecho y los Fundamentos de Derecho anteriores,

RESUELVO

Primero.- Aprobar la Política de Seguridad Interior, Seguridad de las Tecnologías de la Información y Comunicaciones (TIC) y Protección de Datos de la Agencia para la Calidad Científica y Universitaria de Andalucía, en los términos que se especifican en el ANEXO de esta resolución.

Segundo.- Publicar el texto en el Portal Web de la Agencia para la Calidad Científica y Universitaria de Andalucía (ACCUA), así como en el Portal de Transparencia de la misma.

Tercero.- Designar a las personas que componen los miembros del Comité de Seguridad Interior y Seguridad TIC previstos en el Documento de Política de Seguridad Interior, Seguridad TIC y Protección de Datos y a sus correspondientes suplentes.

Cuarto.- La presente resolución surtirá efectos desde el día siguiente al de su aprobación.

EL DIRECTOR

POLÍTICA DE SEGURIDAD INTERIOR, SEGURIDAD DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES (TIC) Y PROTECCIÓN DE DATOS DE LA AGENCIA PARA LA CALIDAD CIENTÍFICA Y UNIVERSITARIA DE ANDALUCÍA

Agencia para la Calidad Científica y Universitaria de Andalucía

Junta de Andalucía | Consejería de Universidad, Investigación e Innovación | Agencia para la Calidad Científica y Universitaria de Andalucía

Índice

1. Introducción.

1.1. Antecedentes.

La Administración de la Junta de Andalucía mediante el Decreto 1/2011, de 11 de enero, modificado por el Decreto 70/2017, de 6 de junio, aprobó la Política de Seguridad de las Tecnologías de la Información y Comunicaciones en la Administración de la Junta de Andalucía, disponiendo que las distintas Consejerías y demás entidades deberán disponer formalmente de sus propias normas específicas de política de seguridad TIC, y adecuar, en su caso, las directrices comunes de la Administración de la Junta de Andalucía a sus particularidades. Asimismo, cada Consejería y entidad deberá contar con un Comité de Seguridad de las Tecnologías de la Información y Comunicación (en adelante, TIC), que actuará como una unidad administrativa especial de dirección y seguimiento en materia de seguridad y con los demás perfiles previstos en el Real Decreto 311/2022, de 3 de mayo , por el que se regula el Esquema Nacional de Seguridad (en adelante, ENS). El ENS se encuentra establecido en el artículo 156.2 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, regulado por el Real Decreto 311/2022, de 3 de mayo, y está constituido por los principio 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. Su finalidad última es la creación de las condiciones necesarias de confianza en el uso de los medios electrónicos, a través de medidas dirigidas a garantizar la seguridad de los sistemas, los datos, las comunicaciones, y los servicios electrónicos, que permitan a la ciudadanía y a las Administraciones Públicas, el ejercicio de derechos y el cumplimiento de deberes a través de estos medios. En este contexto, el ENS exige que todo el sector público cuente con una política de seguridad formalmente aprobada por el órgano competente que ostente las máximas competencias ejecutivas.

Por otro lado, el Decreto 171/2020, de 13 de octubre, por el que se establece la Política de Seguridad Interior en la Administración de la Junta de Andalucía, define un completo sistema de prevención y reacción ante daños en las personas, el patrimonio y el funcionamiento, intencionadamente provocados por agentes externos, personal propio o personas usuarias. Este decreto regula un modelo organizativo funcional en el que por simplificación, eficacia y eficiencia se ha evitado la creación de un Comité de Seguridad Interior, optando por incluir las que hubieran sido sus funciones y tareas entre las de los ya existentes comités de seguridad TIC. En este sentido, en su disposición final primera, modifica el reseñado Decreto 1/2011, de 11 de enero, indicando que “Todas las alusiones en el texto a los «Comités de Seguridad TIC de las entidades» quedan sustituidas por Comités de Seguridad Interior y Seguridad TIC de las Consejerías o entidades dependientes singulares”. Por otra parte, el artículo 10.1 del reseñado Decreto 171/2020, de 13 de octubre, establece que partiendo de sus propios recursos directos, en aquellas entidades dependientes en las que estas lo consideren necesario por virtud del volumen o singularidad de los activos se contará con una Unidad de Seguridad Interior que ejerza la responsabilidad ejecutiva para la seguridad interior de los activos en su ámbito, debiendo ser designada por el Comité de Seguridad Interior y Seguridad TIC.

Por otro lado, la aplicación de la normativa sobre protección de datos de carácter personal supone para la Agencia para la Calidad Científica y Universitaria de Andalucía (en lo sucesivo, ACCUA), en tanto responsable y

también encargada de tratamientos de esta naturaleza, según el caso, que sea necesario la adopción de una serie de medidas de carácter técnico y organizativo tendentes a garantizar los derechos de las personas titulares de dichos datos personales.

En consecuencia, la convergencia de los requisitos de seguridad interior, los referidos requisitos sobre los sistemas de información, y los exigidos para la protección de datos personales hacen aconsejable no acometer acciones desagregadas, que atiendan a cada dimensión por separado, pues ello podría provocar duplicidades, antinomias, confusión y descoordinación internas, además de resultar más oneroso desde el punto de vista de la inversión de recursos humanos, económicos, técnicos y organizativos.

1.2. Objetivo general.

El presente documento tiene por objeto establecer la Política de Seguridad Interior, Seguridad TIC y Protección de Datos (en adelante, la Política) de ACCUA, y el marco organizativo y tecnológico de acuerdo con la normativa reguladora de la Política de Seguridad Interior en la Administración de la Junta de Andalucía, la legislación de seguridad de tecnologías de la información y comunicaciones de la Administración de la Junta de Andalucía, en cumplimiento de la normativa reguladora del ENS y de las disposiciones de protección de datos personales.

Pretende, en definitiva, dirigir y dar soporte a la gestión de la seguridad de la información mediante el establecimiento de una estructura organizativa en la que se apoyará el gobierno de la seguridad, así como de unas directrices básicas de acuerdo a los requisitos propios de seguridad y a la regulación aplicable, constituyéndose en el marco dentro del que se definirá el conjunto de normas reguladoras, procedimientos y prácticas que determinen el modo en que los activos son gestionados, protegidos y distribuidos.

En el ámbito de la seguridad interior, en primer lugar, hay que tener en consideración que las dos sedes con las que cuenta esta Agencia, tanto la sede institucional situada en la ciudad de Córdoba, como la sede de la Secretaría General situada en la ciudad de Sevilla, tienen activos que son utilizados por la Agencia pero cuya gestión y titularidad pertenecen a la Universidad de Córdoba y a la Consejería de Universidad, Investigación e Innovación, respectivamente, lo cual provoca que las facultades de disposición y planificación en este ámbito estén muy limitadas para la Agencia y que básicamente esta se remita a la política de seguridad con carácter general establecida por la Junta de Andalucía y por la establecida con carácter particular por la propia Consejería de adscripción, trasladando a esta última y a la Universidad de Córdoba las necesidades en seguridad interior que surjan en el ámbito de la Agencia en las Comisiones de Coordinación establecidas al efecto. No obstante, este documento tendrá por cometido establecer la estructura organizativa en materia de seguridad con la designación del Comité de Seguridad Interior y Seguridad TIC, así como la designación de la persona responsable en seguridad interior que deba realizar las funciones de carácter ejecutivo determinadas por la normativa para la Unidad de Seguridad Interior. El Comité de Seguridad actuará como unidad de seguimiento y coordinación, y la persona responsable en seguridad interior actuará como enlace para transmitir las necesidades de la Agencia en la comisiones de coordinación de gestión de los edificios en los que se sitúan las oficinas de la Agencia.

En materia de Protección de Datos, se aplicará a los tratamientos de datos personales, total o parcialmente automatizados, así como a los tratamientos no automatizados de datos personales contenidos o destinados a ser incluidos en ficheros de la Agencia, como responsable o encargada de tratamientos.

Lo dispuesto en la Política descrita en este documento, deberá ser observado por todas las personas empleadas públicas de la Agencia, así como por aquellas personas que tengan acceso a sus sistemas de información y a los tratamientos de datos personales que en ellos se gestionan.

La presente resolución se aplica a todas las unidades administrativas de la Agencia y a todas las personas colaboradoras en el ámbito de colaboración con la misma.

1.3. Contexto y obligaciones generales.

ACCUA depende de los sistemas TIC para alcanzar sus objetivos. Estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad o confidencialidad de la información tratada o los servicios prestados.

El objetivo de la seguridad de la información es garantizar la calidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza a los incidentes.

Los sistemas TIC deben estar protegidos contra amenazas de rápida evolución con potencial para incidir en la confidencialidad, integridad, disponibilidad, uso previsto y valor de la información y de los servicios. Para defenderse de estas amenazas, se requiere una estrategia que se adapte a los cambios en las condiciones del entorno para garantizar la prestación continua de los servicios. Esto implica que los departamentos deben aplicar las medidas mínimas de seguridad exigidas por el ENS, así como realizar un seguimiento continuo de los niveles de prestación de servicios, seguir y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados. Los departamentos deben estar preparados para prevenir, detectar, reaccionar y recuperarse de incidentes.

La seguridad de los sistemas de información se abordará aplicando de forma coherente y coordinada esta Política, las normas que la desarrollen y el referente legislativo del ENS a cualquier tipo de información tratada en dichos sistemas, atendiendo a la previsión en materia de seguridad de los datos personales que contiene 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 (en adelante, LOPDGDD).

Las unidades organizativas, entendiéndose por tal los órganos y las unidades administrativas deben cumplir los requisitos mínimos de seguridad exigidos en el ENS. En concreto, los requisitos mínimos son los siguientes:

a) Organización e implantación del proceso de seguridad.

b) Análisis y gestión de los riesgos. En los supuestos de sistemas de información que traten datos personales se realizará, con el asesoramiento de la persona delegada de protección de datos, un análisis de riesgos conforme al artículo 24 del 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 (en adelante, RGPD), en los supuestos de su artículo 35, una evaluación de impacto relativa a la protección de datos.

c) Gestión de personal. Se implantarán los mecanismos necesarios para que cualquier persona que

acceda o pueda acceder a los sistemas de información de la Agencia conozca sus responsabilidades, y de este modo se reduzca el riesgo derivado de un uso indebido de dichos activos.

d) Profesionalidad. La seguridad de los sistemas de información estará atendida, revisada y auditada por personal cualificado.

e) Autorización y control de los accesos. Se limitará el acceso a los activos de información mediante la implantación de los mecanismos de identificación, autenticación y autorización acordes con su calificación.

f) Protección de las instalaciones. Los sistemas de información estarán emplazados en áreas seguras, protegidas por controles de acceso físicos adecuados a su criticidad. Los locales donde se ubiquen los sistemas dispondrán de elementos adecuados para el eficaz funcionamiento del equipamiento allí instalado.

g) Adquisición de productos y contratación de servicios de seguridad. Las diferentes unidades organizativas identificarán los requisitos de seguridad a incluir para la adquisición de productos o contratación de servicios de seguridad.

h) Mínimo privilegio. Otorgar a los usuarios los permisos estrictamente necesarios sobre los sistemas y la información para el desempeño de sus funciones en el organismo según sus perfiles individuales y específicos, eliminando cualquier función innecesaria o inadecuada para conseguir este fin. Las funciones de operación y administración serán desarrolladas exclusivamente por el personal autorizado.

i) Integridad y actualización del sistema. Se requerirá una autorización formal previa a la instalación de un sistema por parte de la persona responsable del servicio de acuerdo con lo dispuesto 5.2.2 de este documento. Se deberá conocer el estado de la seguridad del sistema en relación con las recomendaciones y actualizaciones de seguridad recomendadas por el fabricante.

j) Protección de la información almacenada y en tránsito. Toda la información almacenada de forma centralizada será periódicamente respaldada. La información que se transmita a través de redes de comunicaciones o soportes portátiles estará adecuadamente protegida, teniendo en cuenta su calificación y criticidad, mediante mecanismos que garanticen su seguridad.

k) Prevención ante otros sistemas de información interconectados. Se dispondrá de un sistema de cortafuegos que separe la red interna del exterior. Todo el tráfico atravesará dicho cortafuegos y sólo se dejará transitar los flujos previamente autorizados. Se asegurará la autenticidad del otro extremo de un canal de comunicación antes de intercambiar información alguna.

l) Registro de actividad y detección de código dañino. Se registrarán aquellos eventos que se consideren de interés, tanto para la detección de actividades que puedan comprometer la seguridad, como para dejar constancia de aquellas otras actividades que permitan verificar y evidenciar la efectividad de los controles, las normas de seguridad establecidas por la Agencia y los requisitos legales aplicables.

m) Incidentes de seguridad.

n) Continuidad de la actividad. Las personas responsables del servicio de acuerdo con el apartado

5.2.2. del presente documento, deberán elaborar planes de continuidad del servicio. Se implantarán mecanismos apropiados para asegurar la disponibilidad de los sistemas de información teniendo en cuenta la valoración de la dimensión de disponibilidad.

ñ) Mejora continua del proceso de seguridad. Se elaborarán planes de mejora continua que se presentarán para su aprobación al Comité de Seguridad Interior y Seguridad TIC.

Las unidades organizativas deberán realizar un seguimiento continuo de los niveles de prestación de los servicios, seguir y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados. Las diferentes unidades organizativas deben cerciorarse de que la seguridad TIC es una parte integral de cada etapa del ciclo de vida del sistema, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación. Así, los requisitos de seguridad y las necesidades de financiación deben ser identificados e incluidos en la planificación, en la solicitud de ofertas, y en pliegos de licitación para proyectos TIC. Las unidades organizativas deben estar preparadas para prevenir, detectar, responder y recuperarse de los incidentes de seguridad.

Las reglas de uso de los recursos TIC serán trasladadas convenientemente, en la medida en que pueda resultar necesario o recomendable, al clausulado de los contratos suscritos por la Agencia y a los demás instrumentos jurídicos en los que se vertebre cualquier prestación de servicios TIC a la misma.

La seguridad y la protección de los datos personales estarán presentes durante todo el ciclo de vida. Las personas usuarias están obligadas a guardar secreto profesional de toda aquella información de la que tengan conocimiento con ocasión del ejercicio de su cargo o actividad profesional. Esta obligación se mantendrá incluso después de haber finalizado la relación con la Agencia.

El deber de confidencialidad y secreto profesional se establecerá de forma expresa en todo tipo de relaciones -administrativas, civiles o mercantiles-, que impliquen o supongan acceso o tratamiento de la información, incluidos los servicios de simple alojamiento, transporte o soporte técnico.

En lo referente a Seguridad TIC, se adoptan los principios, objetivos y definiciones establecidos en los artículos 2, 4 y 5 del 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, así como los principios mínimos establecidos en el Real Decreto 311/2022, de 3 de mayo, por el que se regula el ENS. Toda la documentación generada para el desarrollo de proyectos TIC tendrá la obligación de utilización de un lenguaje no sexista.

En lo relativo a Seguridad Interior, se adoptan los objetivos, definiciones y principios definidos en los artículos 3, 4 y 5 del Decreto 171/2020, de 13 de octubre, por el que se establece la Política de Seguridad Interior en la Administración de la Junta de Andalucía. Asimismo, se adoptarán los términos y objetivos establecidos por el Plan de Seguridad Interior de la Consejería de Universidad, Investigación e Innovación aprobado con fecha 15 de noviembre de 2022, o de aquella revisión o plan que lo sustituya.

En lo concerniente a la Protección de Datos Personales, se adoptan igualmente los objetivos, definiciones y principios establecidos en los artículos 1, 4, 5, 6, 7, 8, 9 y 10 del RGPD y los recogidos en los artículos 4, 5, 6, 7, 8, 9, 10 de la LOPDGDD. Asimismo, según los principios aplicados al tratamiento, los datos personales serán tratados de manera lícita, leal y transparente, recogidos con fines determinados, explícitos y legítimos, y no

tratados ulteriormente de manera incompatible con dichos fines. Los datos serán adecuados, pertinentes y limitados (principio de minimización), exactos y actualizados, mantenidos durante no más tiempo del necesario para los fines del tratamiento, y tratados de manera que se garantice una seguridad adecuada incluida la protección contra el tratamiento no autorizado o ilícito y contra su perdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas y organizativas adecuadas (integridad y confidencialidad).

El principio de transparencia por su parte (artículo 12.º del RGPD) exige además el deber al responsable de tomar medidas oportunas para facilitar al interesado toda información relativa a sus tratamientos, sus ejercicios de derechos o violaciones de seguridad en un lenguaje sencillo claro, de forma concisa, transparente, inteligible y de fácil acceso. El responsable del tratamiento además queda obligado al cumplimiento de los principios y derechos anteriores y a su acreditación.

1.4. Prevención.

Los departamentos deben evitar, o al menos prevenir en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad. Para ello, los departamentos deben implementar las medidas mínimas de seguridad determinadas por el ENS y del RGPD.

Los perfiles y responsabilidades de seguridad de todo el personal, deben estar claramente definidos y documentados.

Para garantizar el cumplimiento de la política, los departamentos deben:

1. Autorizar la puesta en funcionamiento de los sistemas TIC de su competencia.
2. Evaluar regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.
3. Solicitar la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

1.5. Detección.

Se realizarán labores de monitorización de los sistemas de manera continua para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia según lo establecido en el ENS, para evitar su rápida degradación debido a incidentes.

Si la anomalía detectada afectase a datos personales, se contactará con el responsable del tratamiento que actuará de acuerdo con lo establecido en la presente orden relativo a la violación de la seguridad de los datos personales.

La monitorización es especialmente relevante cuando se establecen líneas de defensa de acuerdo con lo dispuesto en el ENS. Así, se establecerán mecanismos de detección, análisis y reporte que lleguen a las personas responsables tanto de una manera regular, como cuando se produzca alguna desviación significativa de los parámetros que se hayan preestablecido como normales.

1.6. Respuesta.

Los departamentos deben :

a) Colaborar con el equipo de gestión de incidentes de seguridad de la Agencia y con la persona Delegada de Protección de Datos, en caso de que se vean afectados datos personales.

b) Designar un punto de contacto para las comunicaciones relativas a incidentes detectados en otras unidades organizativas o en otros organismos.

c) Establecer protocolos para el intercambio de información relacionada con el incidente. Esto incluye comunicaciones, en ambos sentidos, con los equipos de respuesta ante emergencias informáticas.

1.7. Recuperación.

Para garantizar la disponibilidad de los servicios críticos, las personas responsables de los servicios deben colaborar en el desarrollo de planes de continuidad de sus sistemas TIC como parte de su plan general de continuidad de negocio y actividades de recuperación liderados por el Comité de Seguridad Interior y Seguridad TIC.

2. Alcance.

Esta política se aplica a los sistemas TIC de ACCUA. Así mismo, se aplica a todos los miembros de la organización, sin excepciones.

3. Misión.

La política de seguridad tiene como misión disminuir de manera significativa los riesgos a los que están sometidos los activos físicos y los activos de información, así como los datos personales que puedan albergarse en estos, y que dan soporte a ACCUA.

4. Marco normativo.

Este documento, con independencia de la legislación complementaria de aplicación, está basado en la siguiente normativa:

- 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 (BOJA número 11, de 18 de enero de 2011).
- Decreto 70/2017, de 6 de junio, por el que se modifica 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 (BOJA número 110, de 12 de junio de 2017).
- Decreto 171/2020, de 13 de octubre, por el que se establece la Política de Seguridad Interior en la Administración de la Junta de Andalucía (BOJA número 201, de 16 de octubre de 2020).
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (BOE número 106, de 4 de mayo de 2022).

- Decreto 574/2022, de 27 de diciembre, por el que se modifica el Decreto 158/2022, de 9 de agosto, por el que se regula la estructura orgánica de la Consejería de Universidad, Investigación e Innovación.
- Decreto 158/2022, de 9 de agosto, por el que se regula la estructura orgánica de la Consejería de Universidad, Investigación e Innovación.
- Ley 9/2021 de 23 de diciembre por la que se crean la Agencia Empresarial para la Transformación y el desarrollo Económico (TRADE) y la Agencia para la Calidad Científica y Universitaria de Andalucía (ACCUA).
- Decreto 17/2023, de 14 de febrero, por el que se aprueban los Estatutos de la Agencia para la Calidad Científica y Universitaria de Andalucía (ACCUA).
- Decreto 289/2015, de 21 de julio, por el que se regula la organización administrativa en materia de transparencia pública en el ámbito de la Administración de la Junta de Andalucía y sus entidades instrumentales (BOJA número 249, de 30 de diciembre de 2022).
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.
- Resolución de 22 de octubre de 2020, de la Secretaría General para la Administración Pública, por la que se aprueba el Código de Conducta en el uso de las Tecnologías de la Información y la Comunicación para profesionales públicos de la Administración de la Junta de Andalucía (BOJA número 208, de 27 de octubre de 2020).
- 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 (Reglamento general de protección de datos).
- Orden de 8 de mayo de 2024, por la que se establece la política de seguridad interior y seguridad de las tecnologías de la información y comunicaciones en el ámbito de la Consejería de Universidad, Investigación e Innovación y de sus entidades adscritas.

5. Organización de la seguridad.

La organización de la seguridad se establece en su conjunto pero con incidencia en distintos ámbitos, por un lado tenemos la seguridad de los activos que podríamos llamar “físicos” que se contemplan bajo el término “seguridad interior” y por otro lado, la seguridad de los activos que son sistemas información. Además, dentro de estos dos ámbitos se pueden albergar datos personales, por lo que la organización de la seguridad también tendrá que contemplar la seguridad de dichos datos.

El mantenimiento y gestión de la seguridad de la información en una entidad va íntimamente ligado al establecimiento de una organización de seguridad. Dicha organización se establece mediante la identificación y definición de las diferentes actividades y responsabilidades en materia de gestión de la seguridad y la implantación de una estructura que las soporte.

La estructura que se define en este documento diferencia tres grandes bloques de responsabilidad en el ámbito de los sistemas de información: i) la especificación de las necesidades o requisitos en materia de seguridad de la información, ii) la operación del sistema de información que se atiene a dichos requisitos y iii) la función de supervisión de acuerdo al principio básico del ENS de “la seguridad como función diferenciada”.

Siguiendo la terminología utilizada en el ENS, la especificación de los requisitos de seguridad corresponderá al responsable de la información y a los responsables de los servicios; y al responsable del tratamiento si hubiera datos de carácter personal. La operación corresponderá al responsable del sistema y, por último, la supervisión corresponderá al responsable de la seguridad.

La seguridad de la información implica prácticamente a todas las áreas de ACCUA, habida cuenta de que ha de estar presente en todos los ámbitos de su actividad y debe tener un carácter multidisciplinar, abarcando áreas como la informática y comunicaciones, gestión de personal y financiera, ejecución de proyectos, actividades de evaluación y acreditación, etc.

La estructura organizativa de la gestión de la seguridad de la Agencia está compuesta por las siguientes figuras:

a) El Comité de Seguridad Interior y Seguridad TIC.

b) La persona Responsable de la Seguridad Interior.

c) La persona Responsable de la Seguridad TIC.

d) La persona Responsable de la Información.

e) Las personas Responsables de los Servicios.

f) La persona Responsable del Sistema.

g) La persona Delegada de Protección de Datos.

Dependiendo de las necesidades y circunstancias de la organización, en ciertos casos la función de algunos de estos agentes podrá recaer sobre una misma persona, unidad o departamento, respetando siempre el principio básico de función diferenciada o bien implementando alguna medida compensatoria cuando sea inevitable (por ejemplo, auditoria externa cada cierto tiempo).

La estructura organizativa será competente para mantener, actualizar y hacer cumplir, dentro del ámbito definido, la política de seguridad de la información.

Además, en el ámbito de la Agencia, las siguientes figuras ostentan atribuciones directamente relacionadas con la seguridad que son las que les asigna la normativa sobre protección de datos de carácter personal:

a) Responsable del Tratamiento de Datos Personales (artículo 4 del RGPD).

b) Encargado del Tratamiento de Datos Personales (artículo 4.8 RGPD).

c) La persona Delegada de Protección de Datos.

A continuación se describe cada una de estas figuras y su objetivo.

5.1. Comité de Seguridad Interior y Seguridad TIC de la Agencia.

5.1.1. Objetivo y miembros.

Se crea el Comité de Seguridad Interior y Seguridad TIC de la Agencia para la Calidad Científica y Universitaria de Andalucía como unidad administrativa especial para la dirección y seguimiento en materia de seguridad interior en todos sus ámbitos de actuación y en materia de seguridad de los activos TIC de los que esta Agencia sea titular o cuya gestión tenga encomendada.

Este Comité estará compuesto por los siguientes miembros:

a) Presidencia: la persona titular de la Dirección.

b) Vicepresidencia: la persona titular de la Secretaría General.

c) Vocalías:

1.º La persona titular de la Jefatura del Área de Evaluación y Acreditación.

2.º La persona titular de la Jefatura del Área de Calidad y Relaciones Institucionales.

d) Secretaría: La persona titular de la Gerencia de la Agencia, con voz y voto.

La persona Delegada de Protección de Datos, la persona Responsable de Seguridad TIC y la persona Responsable del Sistema, en el caso de que no formen parte del Comité como vocales o ejerciendo la Secretaría, asistirán en calidad de asesores a las reuniones del Comité de Seguridad Interior y Seguridad TIC, salvo que puntualmente se disponga lo contrario de forma expresa por parte de la presidencia.

En caso de vacante, ausencia, enfermedad y, en general, cuando concurra una causa justificada, la persona titular de la presidencia podrá ser sustituida por la persona titular de la vicepresidencia. La vicepresidencia, las vocalías y la secretaría podrán ser sustituidas por la persona que designe la presidencia del Comité de Seguridad Interior y Seguridad TIC.

5.1.2. Funciones del Comité de Seguridad Interior y Seguridad TIC.

5.1.2.1. En relación con las funciones de seguridad interior.

Este Comité tendrá asignadas las siguientes funciones:

a) Definir, aprobar y realizar el seguimiento de los objetivos, iniciativas y planes estratégicos para la seguridad interior, incluido el Plan de Seguridad Interior de la Agencia.

b) Impulsar el cumplimiento de la política de seguridad interior.

c) Velar por la disponibilidad de los recursos para el desarrollo de los objetivos e iniciativas definidas en el Plan de Seguridad Interior de la Agencia en coordinación con la Consejería de adscripción.

d) Atender las peticiones en materia de seguridad interior de las diferentes sedes de la Agencia.

e) La designación de la persona Responsable de Seguridad Interior de la Agencia.

f) Promover programas de formación, entrenamiento y concienciación sobre las medidas relativas a la seguridad interior entre el personal de la Agencia.

g) Cualquier otra que se le asigne, por órgano o normativa competente, en materia de seguridad

interior.

5.1.2.2. En relación con la seguridad TIC.

El Comité tendrá asignadas las siguientes funciones:

a) Impulsar el cumplimiento de la política de seguridad TIC y su desarrollo normativo, estableciendo las directrices comunes y de supervisión de seguridad TIC.

b) Definir, aprobar y realizar el seguimiento de los objetivos, iniciativas y planes estratégicos en materia de seguridad TIC, velando, en particular, por la coordinación entre diferentes planes que puedan coexistir, tomando especialmente en consideración el de la Consejería de adscripción. Además, le corresponde promover la mejora continua del sistema de gestión de la seguridad TIC.

c) Velar por la disponibilidad de los recursos necesarios para desarrollar las iniciativas y planes estratégicos definidos en coordinación con la Agencia Digital de Andalucía.

d) Nombrar a la persona Responsable de Seguridad TIC, garantizando en la medida de lo posible el principio de función diferenciada, y en caso contrario, establecer las medidas compensatorias que se estimen convenientes.

e) Nombrar a la persona Responsable del Sistema.

f) Impulsar el cumplimiento de la política de seguridad TIC.

g) Atender las peticiones en materia de seguridad TIC de las diferentes sedes de la Agencia.

h) Informar a la persona titular de la Presidencia de la Agencia del estado de la seguridad de las TIC en el ámbito de la Agencia cuando se produzcan incidencias graves o muy graves de seguridad.

i) Elevar las propuestas de revisión de la política de seguridad TIC de la Agencia, de sus directrices y sus normas de seguridad, así como del marco normativo de seguridad TIC de la Administración de la Junta de Andalucía, a los órganos competentes para su tramitación.

j) Aprobar las normas generales de seguridad TIC de la Agencia en coordinación con la Agencia Digital de Andalucía y la Consejería de adscripción.

k) Coordinar los esfuerzos de todo el equipo humano con responsabilidad en materia de seguridad TIC para asegurar que son consistentes y están alineados con la estrategia decidida, evitando duplicidades.

l) Realizar tareas de coordinación con el Comité de Seguridad Interior y de Seguridad TIC de la Consejería de adscripción.

m) Promover la formación, el entrenamiento y la concienciación de las medidas legales y organizativas relativas a la seguridad TIC entre el personal de la Agencia.

n) Elaborar y aprobar los requisitos de formación y cualificación de las personas administradoras, operadoras y usuarias desde el punto de vista de seguridad TIC de la Agencia.

ñ) Coordinar y aprobar los planes de continuidad de la Agencia.

o) Promover auditorías periódicas para verificar el correcto cumplimiento de la política, la normativa

y los procedimientos de seguridad.

p) Monitorizar los principales riesgos residuales asumidos y recomendar posibles actuaciones respecto de los mismos.

q) Monitorizar el desempeño de los procesos de gestión de incidentes de seguridad y recomendar posibles actuaciones respecto de ellos, velando, en particular, por la coordinación en la gestión de incidentes de la seguridad TIC y por los riesgos que pudiera suponer para los datos personales.

r) Priorizar las actuaciones en materia de seguridad TIC en coordinación con la Agencia Digital de Andalucía cuando los recursos sean limitados.

s) Velar para que la seguridad TIC se tenga en cuenta en todos los proyectos y actividades, desde su especificación inicial hasta su puesta en producción, evitando duplicidades y permitiendo un funcionamiento homogéneo de todo el sistema.

t) Resolver los conflictos de competencia que se puedan suscitar entre las diferentes personas responsables de la gestión de seguridad TIC o elevar propuesta para resolverlos, en su caso.

u) Impulsar la determinación de los niveles de seguridad de la información tratada, en la que se valorarán los impactos que tendrían los incidentes que afectarán a la seguridad de la información, todo ello con la participación de la persona responsable de la información, del Responsable de Seguridad TIC y con el asesoramiento de la persona Delegada de Protección de Datos.

v) Impulsar los preceptivos análisis de riesgos, junto a las personas responsables de la información que correspondan, contando con la participación de la persona Responsable de Seguridad TIC y del asesoramiento de la persona Delegada de Protección de Datos.

w) Coordinar la aceptación de los riesgos residuales por sus responsables correspondientes respecto de la información y servicios de su competencia, obtenidos en los análisis de riesgos realizados.

x) Coordinar las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado, de acuerdo con el correspondiente análisis de riesgo para los derechos y libertades de las personas físicas y, en su caso, las evaluaciones de impacto relativas a la protección de datos personales, contando con el asesoramiento de la persona Delegada de Protección de Datos.

5.1.3. Funcionamiento del Comité de Seguridad Interior y Seguridad TIC.

El Comité de Seguridad Interior y Seguridad TIC se reunirá con carácter ordinario, al menos, una vez al año, y con carácter extraordinario, cuando lo decida la persona titular de la presidencia, de oficio o a propuesta de alguno de sus miembros, y en todo caso cuando se produzca alguno de los siguientes supuestos:

a) Se produzcan incidencias de seguridad graves que afecten a cualquier sistema o a la seguridad interior.

b) Surjan nuevas necesidades de seguridad que requieran la participación del Comité.

El Comité se podrá constituir, convocar, celebrar sus sesiones, adoptar acuerdos y remitir actas, tanto de forma presencial como utilizando redes de comunicación a distancia, con las medidas adecuadas que garanticen la identidad de las personas comunicantes, así como la integridad, confidencialidad y la autenticidad de la información entre ellas transmitidas. Los miembros del Comité están obligados a respetar

la confidencialidad de toda la información a la que tengan acceso.

Los miembros del Comité de Seguridad Interior y Seguridad TIC podrán proponer a la Presidencia, individual o colectivamente, la inclusión de asuntos en el orden del día. La propuesta deberá realizarse a través de medios electrónicos, dirigido a la Presidencia con una antelación mínima de 48 horas a la fecha de la convocatoria.

A las sesiones del Comité de Seguridad Interior y de Seguridad TIC podrán asistir en calidad de asesoras, con voz pero sin voto, las personas que en cada caso estime pertinente la Presidencia, por iniciativa propia o a propuesta de sus miembros.

La presidencia del Comité ostentará voto de calidad en caso de empate en la toma de decisiones.

De todas las sesiones celebradas se levantará un acta con los acuerdos adoptados.

Esta acta tendrá carácter de información reservada dada la naturaleza de las funciones y los contenidos a tratar por el Comité.

El Comité se regirá por este documento, por la normativa reguladora de la política de seguridad de las tecnologías de la información y comunicaciones en la Administración de la Junta de Andalucía, y por la Política de Seguridad Interior en la Administración de la Junta de Andalucía, y por el resto de normativa aplicable, como la reguladora del ENS y la normativa de protección de datos personales.

5.2. Perfiles de responsabilidad.

Las figuras o perfiles de Responsabilidad que se describen en los siguientes epígrafes deben entenderse como un conjunto de responsabilidades y atribuciones que deben quedar adecuadamente cubiertas dentro de la organización, con independencia de a qué persona concreta o conjunto de personas sean asignadas.

5.2.1. Persona Responsable de Seguridad TIC.

De acuerdo con lo establecido en el artículo 13.2.c del ENS, y en el artículo 11 del Decreto 1/2011, de 11 de enero (Política de Seguridad TIC en la Administración de la Junta de Andalucía, modificado por el Decreto 70/2017, de 6 de junio), la Agencia contará con una persona Responsable de Seguridad TIC que ejerza las funciones de responsabilidad de seguridad TIC de la Agencia. La persona responsable de seguridad TIC será nombrada por el Comité de Seguridad Interior y Seguridad TIC.

La persona Responsable de Seguridad TIC tendrá las siguientes atribuciones:

a) Soporte técnico, asesoramiento e información al Comité, así como de ejecución de las decisiones y acuerdos adoptados por éste.

b) Diseño y ejecución de los programas de actuación propios de la Agencia, incluyendo, entre otros, planes directores de seguridad, proyectos de desarrollo normativo, auditorías de cumplimiento y planes de adecuación legal.

c) Delimitación, implantación y mantenimiento de los controles de carácter organizativo para la protección de los datos, aplicaciones y sistemas, así como la realización y mantenimiento de los análisis de riesgos.

d) Supervisión sistemática de los controles de carácter procedimental, operacional y medidas técnicas de protección de los datos, aplicaciones y sistemas de la Agencia.

e) Determinación y supervisión de los criterios y requisitos técnicos de seguridad aplicados en las distintas fases del ciclo de vida de los soportes, sistemas y aplicaciones de la Agencia por parte de los Servicios o unidades responsables de la prestación de los servicios de tecnologías de la información y comunicaciones. Antes de la puesta en producción de nuevos sistemas de información o evolutivos de los existentes, el Responsable de Seguridad TIC deberá evaluar los aspectos de seguridad y comunicar los posibles riesgos a la persona responsable de la Información y a la persona responsable del Servicio.

f) Definición y ejecución de los programas formativos y de concienciación relacionados con buenas prácticas de seguridad TIC en el ámbito de la Agencia, procurando promover, en el proceso de selección de las personas participantes en estos programas, la concurrencia de mujeres.

La persona responsable de seguridad TIC elaborará y mantendrá un inventario de servicios y sistemas en el que se indiquen expresamente las personas u órganos nombrados por el Comité, que asumen las figuras de responsable de la información, responsable del servicio, y responsable del sistema. En aquellos servicios y sistemas que traten datos de carácter personal y en coordinación con la persona Delegada de Protección de Datos, deberán ser identificados los tratamientos de datos personales realizados por o encomendados a la Agencia, y las unidades administrativas u organismos que asumen las figuras de responsable del tratamiento y encargado del tratamiento.

5.2.2. Responsable de la Información y de los Servicios.

La persona responsable de la información es la persona titular de la Dirección, quien decide sobre la finalidad, contenido y uso de la información de cada sistema de información

Las personas responsables de los servicios serán las personas titulares de las jefaturas de área y la persona titular de la Secretaría General,quienes deciden sobre las características del servicio a prestar por cada sistema de información.

Las funciones de los responsables de la información y de los servicios serán las siguientes:

a) Asistir a la determinación de los requisitos de seguridad TIC, categorizando la información/los servicios mediante la valoración de los impactos de los incidentes que puedan producirse.

b) Proporcionar la información necesaria a la persona Responsable de Seguridad TIC para realizar los preceptivos análisis de riesgos TIC, con la finalidad de establecer las salvaguardas a implantar. Para ello contarán con la colaboración de la persona Responsable del Sistema.

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

d) Aceptar los riesgos residuales de las informaciones tratadas y los servicios prestados, identificados en el análisis de riesgos y realizar su seguimiento y control.

5.2.3. Responsable del tratamiento de datos personales.

El responsable del tratamiento de datos personales en el ámbito de aplicación de esta política es la persona titular de la Dirección de la Agencia ACCUA.

5.2.4. Encargados del tratamiento de datos personales.

Las principales funciones y responsabilidades de los encargados del tratamiento, dentro de su ámbito de actuación, son las establecidas en el artículo 28 del RGPD y demás normativa de aplicación.

De conformidad con el artículo 28 del RGPD cuando se vayan a tratar datos personales por cuenta de un responsable, este elegirá únicamente un encargado que ofrezca garantías suficientes para aplicar medidas técnicas y organizativas apropiadas, de manera que el tratamiento garantice la protección de los derechos de la persona interesada. El tratamiento por el encargado se regirá por un contrato u otro acto jurídico que vincule al encargado respecto del responsable y establezca el objeto, la duración, la naturaleza y la finalidad del tratamiento, el tipo de datos personales y categorías de interesados, y las obligaciones y derechos del responsable. Dicho contrato o acto jurídico constará por escrito, inclusive en formato electrónico.

El encargado del tratamiento, y cualquier persona que actúe bajo la autoridad de la persona responsable o encargada del tratamiento, y que tenga acceso a datos personales, solo podrá tratar dichos datos siguiendo instrucciones documentadas del responsable, a no ser que estén obligados a ello en virtud de normativa aplicable.

5.2.5. La persona Delegada de Protección de Datos.

La persona delegada de protección de datos personales será designada atendiendo a sus cualidades profesionales y, en particular, a sus conocimientos especializados del Derecho y la práctica en materia de protección de datos, de conformidad con lo establecido en los artículos 37 del RGPD y 35 de la LOPDGDD. En la designación deberá especificarse el alcance de la misma, indicando los responsables del tratamiento para los que ejercerá sus funciones.

El responsable y el encargado del tratamiento garantizarán que la persona delegada de protección de datos no reciba ninguna instrucción en lo que respecta al desempeño de dichas funciones, de acuerdo con el artículo 38.3 del RGPD. No será destituida ni sancionada por el responsable o el encargado por desempeñar sus funciones, salvo que incurriera en dolo o negligencia grave en su ejercicio.

La designación, nombramiento y cese de la persona delegada de protección de datos deberá comunicarse en el plazo de diez días al Consejo de Transparencia y Protección de Datos de Andalucía.

5.2.6. Persona Responsable del Sistema.

Será responsable del sistema la persona que dirija el desarrollo y mantenimiento de los sistemas de información durante todo su ciclo de vida.

Las funciones del responsable del sistema serán las siguientes:

a) Gestionar el sistema durante todo su ciclo de vida, desde la especificación de este a la instalación y seguimiento de su funcionamiento.

b) Velar porque la seguridad TIC esté presente en todas y cada una de las partes del ciclo de vida del sistema contemplando que las directrices de seguridad establecidas de manera horizontal por la Junta de Andalucía se sigan en el desarrollo del sistema.

c) Implementar las medidas de seguridad de los sistemas de información y supervisar su correcto funcionamiento en la operación diaria.

d) Verificar de forma previa a su publicación, que existen y están actualizadas las cláusulas y requisitos de seguridad particulares especificados por la persona Responsable de Seguridad TIC, en los posibles contratos relacionados con el sistema, y posteriormente durante el desarrollo del sistema deberá verificar su cumplimiento. Para ello podrá contar con el asesoramiento de la Unidad de Seguridad TIC Corporativa.

e) Asesorar en la definición de la tipología y política de gestión del sistema, definiendo los criterios de uso y los servicios disponibles en el mismo.

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

g) Crear y gestionar la documentación de seguridad del sistema, con el asesoramiento de la persona Responsable de Seguridad TIC.

h) Asesorar, en colaboración con la persona Responsable de Seguridad TIC, a los responsables de la información y a los responsables de los servicios en el proceso de análisis y la gestión de riesgos.

i) Investigar los incidentes de seguridad que afecten al sistema, y en su caso, comunicarlos a la persona Responsable de Seguridad o a quién éste determine. En aquellos que afecten a los derechos y libertades comunicarlo al Responsable o Encargado del Tratamiento y a la persona Delegada de Protección de Datos.

j) Suspender el tratamiento de cierta información o la prestación de un determinado servicio si detecta deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos. Esta decisión debe ser acordada con la persona Responsable de Seguridad TIC y con las personas responsables del servicio y de la información involucradas, antes de ser ejecutada.

Estas tareas se realizarán en colaboración con otras áreas de la Agencia que puedan dar soporte al sistema de información, y contarán con el apoyo de dichas áreas para la implantación de las medidas de seguridad.

5.3. Actualización de la política de seguridad de la información.

Una de las funciones del Comité de Seguridad Interior y Seguridad TIC de la Agencia consistirá en la revisión anual de esta política de seguridad de la información y la propuesta de revisión o mantenimiento de la misma. Las modificaciones en la política de seguridad serán aprobadas por la persona titular de la Agencia y difundidas a través de los medios que se establezcan por el Comité de Seguridad Interior y Seguridad TIC.

6. Datos personales.

Todos los sistemas de información de la Agencia se ajustarán a lo exigido por el RGPD y a la LOPDGDD, así como por el resto de la normativa general o sectorial de protección de datos personales que sea de aplicación.

Todos los tratamientos de datos personales, automatizados o no automatizados, se sujetarán a la citada normativa cuando se encuentren dentro de su ámbito de aplicación.

7. Gestión de riesgos.

ACCUA realizará una gestión de la seguridad basada en los riesgos, propiciando que tanto el análisis como la gestión de riesgos sean parte esencial del proceso de seguridad, que deberá ser lo más transversal posible al resto de procesos de la organización.

En los supuestos de sistemas de información que traten datos personales, el responsable o el encargado del tratamiento, asesorado por la persona Delegado de Protección de Datos, realizarán un análisis de riesgos conforme al artículo 24 del RGPD.

La gestión de riesgos deberá realizarse de manera continua sobre cada sistema de información, conforme a los principios de gestión de la seguridad basada en los riesgos y reevaluación periódica. Dicha gestión permitirá mantener un entorno controlado, minimizando los riesgos hasta niveles aceptables, reduciendo estos niveles mediante el despliegue de medidas de seguridad, proceso para el que se establecerá un equilibrio entre la naturaleza de los datos y los tratamientos, los riesgos a los que estén expuestos y las medidas de seguridad.

El proceso de gestión de riesgos comprende las fases de identificación y valoración de las informaciones y los servicios esenciales prestados, la categorización de los sistemas, el análisis de riesgos y la selección de las medidas de seguridad a aplicar, las cuales deberán estar justificadas y ser proporcionales a los riesgos.

Las personas responsables de la información y las personas responsables del servicio serán responsables de los riesgos sobre la información y de los servicios respectivamente; y por tanto, de aceptar los riesgos residuales calculados en el análisis de riesgos, así como de realizar su seguimiento y control, sin perjuicio de la posibilidad de delegar esta tarea.

El responsable del tratamiento, teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento, será responsable de analizar los riesgos para los derechos y libertades de las personas físicas que conlleven los tratamientos de datos personales de los que sea responsable y aplicará las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo.

El Comité de Seguridad Interior y Seguridad TIC será responsable de realizar un seguimiento de los principales riesgos residuales asumidos por la organización y de recomendar posibles actuaciones respecto de ellos.

La selección de las medidas de seguridad a aplicar, así como el seguimiento de su aplicación, será propuesta por la persona Responsable de Seguridad TIC.

Al menos una vez al año se realizará por parte de la persona Responsable de Seguridad un análisis de riesgos.

Además, se realizará un análisis de riesgos cuando se produzcan los siguientes supuestos:

a) Cuando cambie la información manejada.

b) En el momento en que se modifiquen los servicios prestados.

c) En el tiempo en que ocurra un incidente grave de seguridad.

d) Cuando se detecten vulnerabilidades graves.

e) Cuando se determine de forma motivada por el Comité de Seguridad Interior y Seguridad TIC.

La persona Responsable de Seguridad TIC elevará el informe correspondiente al análisis realizado, al Comité

de Seguridad Interior y Seguridad TIC.

Para realizar el análisis de riesgos se utilizará las metodologías y las herramientas que apliquen, de acuerdo con lo establecido en el ENS.

Para la armonización de los análisis de riesgos, el Comité de Seguridad Interior y Seguridad TIC establecerá una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados. El Comité de Seguridad Interior y Seguridad TIC propiciará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

8. Categorización de los sistemas.

La determinación de la categoría de un sistema se realizará de acuerdo a lo que el ENS establezca al respecto.

9. Desarrollo normativo de la política de seguridad.

La política de seguridad complementa los documentos de seguridad de la Agencia en materia de protección de datos de carácter personal, de sistemas de información y de seguridad física de las instalaciones.

Esta política se desarrollará por medio de una normativa de seguridad que afronte aspectos específicos. La normativa de seguridad estará a disposición de todos los miembros de la organización que necesiten conocerla, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones.

El cuerpo normativo sobre seguridad TIC es de obligado cumplimiento y se desarrollará en tres niveles, según el ámbito de aplicación y nivel de detalle técnico, de manera que cada norma de un determinado nivel de desarrollo se fundamente en las normas de nivel superior. Dichos niveles de desarrollo normativo son los siguientes:

a) Primer nivel normativo: Política de Seguridad TIC, directrices y normas generales de seguridad TIC.

b) Segundo nivel normativo: Normas Específicas de Seguridad TIC, que desarrollan y detallan la Política de Seguridad TIC, centrándose en un área o aspecto determinado.

c) Tercer nivel normativo: Procedimientos, procesos, guías e instrucciones técnicas de seguridad TIC, que dan respuesta, incluyendo detalles de implementación y tecnológicos, a cómo se puede realizar una determinada tarea cumpliendo con lo expuesto en la política de seguridad TIC.

Además de los documentos citados en el anterior párrafo, la documentación de seguridad TIC de los órganos contemplados en el ámbito de aplicación de esta norma podrá contar, bajo criterio de la persona Responsable de Seguridad TIC, con otros documentos de carácter no vinculante: recomendaciones, buenas prácticas, informes, registros, evidencias electrónicas, etc.

La persona Responsable de Seguridad TIC deberá mantener la documentación de seguridad actualizada y organizada, y gestionar los mecanismos de acceso a la misma.

El Comité de Seguridad Interior y Seguridad TIC establecerá los mecanismos necesarios para publicar y compartir la documentación derivada del desarrollo normativo con el propósito de normalizarlo, en la medida de lo posible, en todo el ámbito de aplicación de la Política de Seguridad.

10. Gestión de incidentes de seguridad y de la continuidad.

El Comité de Seguridad Interior y Seguridad TIC deberá aprobar y revisar periódicamente un plan para mantener la continuidad de los procesos y sistemas críticos y garantizar su recuperación en caso de desastre. La finalidad de este plan es reducir el tiempo de indisponibilidad a niveles aceptables mediante la combinación de controles de carácter organizativo, tecnológico y procedimental tanto preventivos como de recuperación.

A los efectos de una mejor gestión de los incidentes, se actuará de forma coordinada con el centro especializado y orientado a la prevención, detección y respuesta a incidentes y amenazas de seguridad en el ámbito de la Administración, el sector empresarial y la ciudadanía de la Comunidad Autónoma de Andalucía.

Durante la gestión de los incidentes de seguridad se analizará si han sido afectados datos personales, en cuyo caso se actuará de acuerdo con lo previsto en la presente Política relativo a la violación de la seguridad de los datos personales.

11. Concienciación y formación. Obligaciones del personal.

La seguridad de la información afecta a todas las personas que prestan servicios en la Agencia y a todas las actividades, de acuerdo con el principio de seguridad integral recogido en el artículo 6 del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad. El objetivo consiste en lograr la plena conciencia de estas personas, así como la articulación de los medios necesarios para que todas las personas que intervienen en el proceso y sus responsables jerárquicos tengan una sensibilidad hacia los riesgos que pueden acaecer. Adicionalmente, las personas con responsabilidad en el uso, operación y administración de sistemas TIC deberán haber recibido formación en el manejo seguro de los sistemas, en la medida en que la necesiten para realizar sus funciones.

Todas las personas que presten sus servicios en ACCUA tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y la normativa de seguridad, siendo responsabilidad del Comité de Seguridad Interior y Seguridad TIC disponer los medios necesarios para que la información llegue a los afectados.

Todo el personal de ACCUA asistirán de forma obligatoria a las sesiones de formación en materia de seguridad que la Agencia convoque.

12. Terceras partes.

Cuando ACCUA preste servicios a otros organismos o maneje información de otros organismos, se les hará partícipes de esta Política de Seguridad de la Información, estableciéndose canales para la comunicación y coordinación de los respectivos Comités de Seguridad Interior y Seguridad TIC, y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad y violaciones de seguridad de los datos personales.

Cuando ACCUA utilice servicios de terceros o ceda información a terceros, se les hará partícipes 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 comunicación y resolución de incidencias. Se garantizará que el personal de terceros esté adecuadamente concienciado en

materia de seguridad, al menos al mismo nivel que el establecido en esta Política. Las terceras partes cuyos servicios sean utilizados por la Agencia o a los que esta les ceda o comunique información estarán sujetos al deber de confidencialidad de acuerdo con el artículo 5.1 de la LOPDGDD, en relación con el artículo 5.1.f) del RGPD.

Cuando algún aspecto de la política de Seguridad TIC no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, la persona Responsable de Seguridad TIC requerirá un informe que precise los riesgos en que se incurre y la forma de tratarlos. Se requerirá la aprobación de este informe por los responsables de la información y los servicios afectados antes de continuar con las actuaciones.

13. Auditorías y conformidad normativa.

La Agencia para la Calidad Científica y Universitaria de Andalucía auditará los sistemas de información de forma periódica con objeto de revisar el cumplimiento normativo vigente, así como el cumplimiento en materia de protección de datos, en aquellos sistemas de información que traten datos personales.

Los sistemas de información de ACCUA serán objeto, al menos cada dos años, de una auditoría regular ordinaria interna o externa que verifique el cumplimiento de los requisitos del ENS y de cualquier otra norma que requiera la realización de auditorías periódicas. La persona Responsable de Seguridad TIC coordinará estas actividades de auditoría, y analizará y elevará al Comité de Seguridad Interior y Seguridad TIC (y a la persona Delegada de Protección de Datos, si las conclusiones afectan a los datos personales) las conclusiones que procedan para que éste adopte las medidas correctoras adecuadas.

Con carácter extraordinario deberán realizarse auditorías siempre que se produzcan modificaciones sustanciales en un sistema de información con un potencial impacto en el cumplimiento de las medidas de seguridad.

Los informes de auditoría quedarán a disposición de la persona titular de la Agencia y del Comité de Seguridad Interior y Seguridad TIC.

14. Resolución de conflictos.

En caso de conflicto entre los diferentes responsables, este será resuelto por el órgano superior jerárquico de los mismos. En defecto de lo anterior, prevalecerá la decisión del Comité de Seguridad Interior y Seguridad TIC.

En los conflictos entre las personas responsables que componen la estructura organizativa de la política de seguridad TIC y las personas responsables definidas en virtud de la normativa de protección de datos personales prevalecerá la decisión que presente un mayor nivel de exigencia respecto a la protección de los datos personales.

15. Aprobación y entrada en vigor.

Texto aprobado por la persona titular de la Dirección de la Agencia para la Calidad Científica y Universitaria de Andalucía. Este documento se publicará en la intranet corporativa.

Esta Política de Seguridad de la Información es efectiva desde dicha fecha y hasta que sea reemplazada por una nueva Política.

16. ANEXO I. Composición del Comité de Seguridad Interior y Seguridad TIC de la Agencia.

Cargo dentro del Comité de Seguridad Interior y Seguridad TIC	Recae sobre
Presidencia	Persona titular de la Dirección
Vicepresidencia	Persona titular de la Secretaría General
Vocales	Las personas titulares de las Áreas de Evaluación y Acreditación, y Calidad y Relaciones Institucionales.
Secretaría	Persona titular de la Gerencia

17. ANEXO II. Documentación de seguridad.

Ámbito	Nombre documento	Ubicación
Seguridad TIC	Política de seguridad de ACCUA	Intranet corporativa
Protección de datos	Documento de seguridad ACCUA	Intranet corporativa
Seguridad interior	Plan de Seguridad Interior de ACCUA	Intranet corporativa