3. Otras disposiciones

CONSEJERÍA DE EMPLEO, FORMACIÓN Y TRABAJO AUTÓNOMO

Resolución de 21 de diciembre de 2021, del Servicio Andaluz de Empleo, por la que se aprueba la Política de Seguridad TIC y de Protección de Datos de Carácter Personal en el ámbito de la Agencia.

Mediante la Resolución de la Presidencia del Servicio Andaluz de Empleo, de 25 de junio de 2019, se aprobó formalmente la política de seguridad TIC, así como las disposiciones de desarrollo que adecuaban, en su caso, las directrices comunes de la Administración de la Junta de Andalucía en esta materia a sus particularidades, así como la de contar con un Comité de Seguridad TIC, en desarrollo de lo previsto en el Decreto 1/2011, de 11 de enero, por el que se establece la política de seguridad de las tecnologías de la información y comunicaciones en la Administración de la Junta de Andalucía, modificado por el Decreto 70/2017, de 6 de junio.

Asimismo, en la referida orden, se estableció la política de seguridad TIC de la Agencia definiendo criterios básicos para el tratamiento de datos de carácter personal, asentando el marco normativo de seguridad y la estructura organizativa y de gestión que velaría por su cumplimiento.

La experiencia acumulada y atendiendo a los principios de simplificación, economía, eficacia y eficiencia administrativa, se hace necesaria aprobar una nueva política de seguridad TIC, en aras a su adaptación a lo estipulado en el artículo 11 del 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, por el que se establecen los requisitos mínimos de la seguridad (anexo). Igualmente, se conviene adaptar aspectos organizativos y de funcionamiento del Comité de Seguridad TIC, así como de sus órganos de coordinación y gestión de la Seguridad.

Desde esta óptica, en aras de un mayor claridad, agilidad administrativa y seguridad jurídica, y con la finalidad de una aplicación más eficaz, se considera necesario derogar la Resolución de la Presidencia del Servicio Andaluz de Empleo, de 25 de junio de 2019, por la que se aprueba la política de seguridad TIC, y aprobar una nueva política de Seguridad TIC en el ámbito del Servicio Andaluz de Empleo.

En su virtud, a propuesta de la Dirección-Gerencia, en uso de las atribuciones que me vienen conferidas por el artículo 7 de la Ley 4/2002, de 16 de diciembre, de creación del Servicio Andaluz de Empleo; el artículo 10.2.o) del Decreto 96/2011, de 19 de abril, por el que se aprueba los Estatutos del Servicio Andaluz de Empleo; el artículo 10.2 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; el Decreto 530/2019, de 12 de febrero, por el que se dispone el nombramiento de la persona titular de la Viceconsejería de Empleo, Formación y Trabajo Autónomo, y en el Decreto 100/2019, de 12 de febrero, por el que se regula la estructura orgánica de la Consejería de Empleo, Formación y Trabajo Autónomo,

R E S U E L V O

Primero. Derogar la Resolución de la Presidencia del Servicio Andaluz de Empleo, de 25 de junio de 2019, por la que aprueba la Política de Seguridad TIC.

Segundo. Aprobar la Política de Seguridad TIC y de Protección de Datos de Carácter Personal de la Agencia Servicio Andaluz de Empleo, que se incorpora a esta resolución.

00253156

Tercero. Publicar el texto en el Portal web de la Agencia Servicio Andaluz de Empleo, así como en el subgrupo Seguridad TIC y Protección de Datos de Red Profesional.

Cuarto. La presente resolución surtirá efectos desde el mismo día de su aprobación.

Quinto. Ordenar la publicación de la presente resolución y su anexo en el Boletín Oficial de la Junta de Andalucía.

Sevilla, 21 de diciembre de 2021.- El Presidente, Miguel Ángel García Díaz.

POLÍTICA DE SEGURIDAD TIC Y DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL DEL SERVICIO ANDALUZ DE EMPLEO

1. Objeto.

El presente documento tiene por objeto establecer la política de seguridad de las Tecnologías de la Información y Comunicaciones y de protección de datos de carácter personal (en adelante, seguridad TIC) en el ámbito del Servicio Andaluz de Empleo (en adelante, SAE), así como el marco organizativo y tecnológico de acuerdo con la normativa reguladora de la política de seguridad de las tecnologías de la información y comunicaciones de la Administración de la Junta de Andalucía, en el marco de la normativa reguladora del Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (en adelante, ENS), y de la normativa en materia de protección de datos de carácter personal.

La política de seguridad TIC se aplicará a todos los sistemas de información que son responsabilidad del SAE para el ejercicio de las competencias que tiene atribuidas. Asimismo, deberá ser observada por todo el personal de la Agencia, así como por aquellas personas que tengan acceso a sus sistemas de información.

2. Objetivos, principios y definiciones.

Se adoptan los principios, objetivos y definiciones establecidos en los artículos 2, 4 y 5 del Decreto 1/2011, de 11 de enero, limitado al ámbito competencial de la Agencia SAE.

3. Organización y gestión de la seguridad TIC.

La estructura organizativa de la gestión de la seguridad TIC de la Agencia, en relación con el Esquema Nacional de Seguridad en el ámbito de la administración electrónica, está compuesta por las siguientes figuras:

a) El Comité de Seguridad de las Tecnologías de la Información y Comunicaciones, en adelante Comité de Seguridad TIC y el Grupo de Respuesta a Incidentes en los Sistemas de Información.

b) Unidad de Seguridad TIC, la persona responsable de esta Unidad tendrá la condición de Responsable de Seguridad TIC.

c) Responsables de la Información.

d) Responsables del Sistema.

e) Responsables del Servicio.

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

a) Responsables de los Tratamientos de datos de carácter personal.

b) Encargados de los Tratamientos de datos de carácter personal.

c) El Delegado de Protección de Datos, en adelante DPD.

00253156

4. Creación del Comité de Seguridad de las Tecnologías de la Información y Comunicaciones.

Se crea el Comité de Seguridad de las Tecnologías de la Información de la Agencia del Servicio Andaluz de Empleo, en adelante Comité de Seguridad TIC.

El Comité de Seguridad TIC actuará como órgano de dirección y seguimiento en materia de seguridad de los activos TIC de titularidad del SAE o cuya gestión tenga encomendada.

4.1. Funciones del Comité de Seguridad TIC.

Al Comité le corresponde aplicar, en el ámbito de la Agencia, las previsiones contenidas en la normativa reguladora del Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, y en 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 determinar la política de seguridad que se ha de emplear en la utilización de los medios electrónicos que permita la adecuada protección de la información. En particular, le corresponde:

a) Aprobar el desarrollo de la política de seguridad TIC.

b) Velar por la concienciación y formación del personal en materia de seguridad TIC.

c) Planificar y priorizar las iniciativas necesarias para cumplir con las directrices, los objetivos y los principios básicos marcados en la presente política de seguridad TIC.

d) Proporcionar los medios y recursos necesarios para posibilitar la realización de las iniciativas planificadas.

e) Coordinar a alto nivel todas las actuaciones de seguridad, velando para que la definición y el desarrollo de las mismas se adecuen en todo momento a las directrices marcadas por la política de seguridad TIC, involucrando a las diferentes áreas implicadas.

f) Velar para que todos los ámbitos de responsabilidad y actuación en relación a la seguridad TIC y su tratamiento queden perfectamente definidos, aprobando los nombramientos necesarios para ello. Especialmente, para asegurar que todos y cada uno de los miembros de la estructura de seguridad definida conozcan sus funciones y responsabilidades.

g) Velar porque la seguridad TIC se tenga en cuenta en todos los proyectos TIC desde su especificación inicial hasta su puesta en operación. En particular deberá velar por la creación y utilización de servicios horizontales que reduzcan duplicidades y apoyen un funcionamiento homogéneo de todos los sistemas TIC.

h) Asegurar que el desarrollo normativo que tenga incidencia en el desarrollo o explotación de sistemas de información se adecua a lo establecido en la política de seguridad TIC.

i) Resolver los conflictos que puedan aparecer entre las diferentes personas responsables o entre diferentes áreas de la organización en materia de seguridad TIC.

j) Coordinar las medidas técnicas y organizativas establecidas en la normativa de protección de datos personales, de acuerdo con los correspondientes análisis de riesgos y, en su caso, las evaluaciones de impacto en la protección de datos, contando con el asesoramiento del DPD.

k) Elevación de propuestas de revisión de la política de seguridad TIC, así como de las directrices y normas de seguridad del SAE, o del marco normativo de seguridad TIC de la Junta de Andalucía, a los órganos competentes para su reglamentaria tramitación.

l) Coordinación con el Comité de Seguridad TIC de la Consejería competente en materia de empleo.

4.2. Composición del Comité de Seguridad TIC.

El Comité de Seguridad TIC estará compuesto por los siguientes miembros:

Presidencia: Dirección-Gerencia.

Vocalías: Las personas titulares de los Centros Directivos, así como de la Secretaría General y de la Coordinación de la Dirección-Gerencia.

Una persona en representación de los órganos periféricos de la Agencia SAE, designada por la persona titular de la Presidencia, y que puede ser de carácter rotativo.

00253156

Secretaría: La persona titular de la Jefatura del Servicio de Informática, con voz y voto. En los casos de vacante, ausencia, enfermedad u otra causa legal, será sustituida por una persona funcionaria adscrita al Servicio de Informática, que designe la Presidencia del Comité de Seguridad TIC.

Asimismo, se podrá invitar a una persona representante del Comité de Seguridad TIC de la Consejería con competencias en materia de empleo, con voz pero sin voto.

En caso de vacante, ausencia, enfermedad u otras causas legales, la persona titular de la Presidencia será sustituida por la persona vocal titular del Comité que tenga mayor jerarquía, antigüedad en el órgano y edad, por ese orden, de entre sus componentes.

Al respecto de las vocalías, en caso de vacante, ausencia o enfermedad, la Presidencia podrá designar una persona que les sustituya en estas circunstancias entre personal funcionario que ocupen puestos de trabajo de nivel 28 o superior.

En la composición del Comité ha de garantizarse, en la medida de lo posible, la representación paritaria de mujeres y hombres, conforme a lo establecido en el artículo 19.2 de la Ley 9/2007, de 22 de octubre, y a la definición de representación equilibrada contenida en el artículo 3.3 de la Ley 12/2007, de 26 de noviembre, para la Promoción de la Igualdad de Género en Andalucía.

La persona titular de la Unidad de Seguridad TIC y la persona que ostente la condición de Delegado de Protección de Datos asistirán en calidad de asesores a las reuniones del Comité de Seguridad TIC, salvo que puntualmente se disponga lo contrario de forma expresa por parte de la presidencia. El Comité de Seguridad TIC podrá convocar a sus reuniones a las personas que en cada caso autorice la presidencia, por propia iniciativa o a propuesta de alguno de sus miembros. Asimismo, podrá recabar de personal técnico especializado, propio o externo, la información pertinente para la toma de decisiones.

4.3. Funcionamiento y régimen jurídico del Comité de Seguridad TIC.

El Comité de Seguridad TIC se reunirá con carácter ordinario una vez al año y con carácter extraordinario por acuerdo de la presidencia, a iniciativa propia o previa solicitud razonada de uno de sus miembros.

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 y la autenticidad de la información entre ellas transmitida, de conformidad con lo establecido en el artículo 91.3 de la Ley 9/2007, de 22 de octubre.

El Comité de Seguridad TIC 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, así como por el resto de normativa aplicable, como la reguladora del ENS y la normativa de protección de datos de carácter personal.

La primera reunión del Comité de Seguridad TIC tendrá por objeto la constitución del mismo y se celebrará en un plazo máximo de un mes a partir de la entrada en vigor del presente documento. En dicha reunión constitutiva se procederá al nombramiento la Unidad de Seguridad TIC, mediante la designación de su persona responsable y al nombramiento de los Responsables de la Información y de los Servicios.

5. Grupo de Respuesta a Incidentes en los Sistemas de la Información.

El Comité de Seguridad TIC nombrará un Grupo de Respuesta a Incidentes en los Sistemas de Información, cuya función será la toma urgente de decisiones en caso de contingencia grave que afecte a la seguridad de los sistemas de información críticos del SAE. Será la persona titular del Servicio de Informática quien determine la existencia de tales contingencias y las califique como graves. Las decisiones adoptadas por este grupo serán ratificadas por el Comité en su conjunto cuando sea necesario.

5.1. Composición.

La composición mínima de este grupo será la siguiente:

Presidencia: Dirección-Gerencia.

00253156

Vocalías: Las personas titulares de los Centros Directivos.
Secretaría: La persona titular de la Jefatura del Servicio de Informática.
En el ejercicio de las funciones del grupo participarán en calidad de asesores:
a) La persona responsable de la Unidad de Seguridad TIC.
b) La persona que ostente la condición de Delegado de Protección de Datos.
Su composición podrá ser modificada mediante acuerdo del Comité de Seguridad TIC.

Corresponde al Grupo de Respuesta a Incidentes en los Sistemas de Información, entre sus funciones, notificar a la autoridad competente en materia de seguridad de las redes y sistemas de información los incidentes de seguridad TIC, en los casos y en los términos que determine la normativa aplicable.

La notificación mencionada en el apartado anterior podrá realizarse bien directamente, bien a través de AndalucíaCERT o por el medio o procedimiento que disponga la política de seguridad de las tecnologías de la información y comunicaciones de la Junta de Andalucía que determine la Dirección General competente en materia de coordinación y ejecución de las políticas de seguridad de los sistemas de información y telecomunicaciones de la Administración de la Junta de Andalucía o el Comité de Seguridad TIC corporativo de la Junta de Andalucía.

El SAE estará integrado en el grupo atendido del Centro de Seguridad TIC AndalucíaCERT.

6. Unidad de Seguridad TIC.

La Agencia, de acuerdo con lo establecido en el artículo 11.1 del Decreto 70/2017, de 6 de junio, contará con una Unidad de Seguridad TIC, garantizando el principio de función diferenciada recogido en el artículo 5.j) del Decreto 1/2011, de 11 de enero, que ejerza las funciones de Responsabilidad de Seguridad TIC del SAE, debiendo ser designada la persona responsable de la citada Unidad por el Comité de Seguridad TIC.

La Unidad de Seguridad TIC tendrá las siguientes atribuciones, de acuerdo con lo dispuesto en el art. 11.1 del Decreto 1/2011, de 11 de enero:

a) Labores de soporte, asesoramiento e información al Comité de Seguridad TIC de la Agencia, así como de ejecución de las decisiones y acuerdos adoptados por este.

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

c) Definición, 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 del SAE.

e) Definición 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 Departamentos 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 de evolutivos de los existentes, la Unidad de Seguridad TIC deberá evaluar los aspectos de seguridad y comunicar los posibles riesgos al Responsable de la Información y 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.

g) Aplicación de los criterios y directrices de gestión de la seguridad TIC emanadas de la Unidad de Seguridad TIC Corporativa.

h) Cuantas otras le sean encomendadas por el órgano directivo del SAE del que dependa funcional u orgánicamente.

00253156

7. Responsable de Seguridad TIC.

La persona responsable de la Unidad de Seguridad TIC del SAE tendrá la condición de Responsable de Seguridad TIC, en los términos establecidos en la normativa reguladora del Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

8. Responsables de la Información.

Los responsables de la Información serán los titulares de los Centros Directivos que decidan sobre la finalidad, contenido y uso de la información.

Las principales funciones, dentro de su ámbito de actuación, son las siguientes:

a) Ayudar a determinar los requisitos de seguridad TIC, categorizando la información mediante la valoración de los impactos de los incidentes que puedan producirse.

b) Proporcionar la información necesaria a la Unidad de Seguridad TIC para realizar los preceptivos análisis de riesgos, con la finalidad de establecer las salvaguardas a implantar. Para ello contará con la ayuda de los responsables de los Servicios y de las personas responsables de los Sistemas.

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

9. Responsables de los Servicios.

Los responsables de los Servicios serán los titulares de los Servicios de gestión que decidan sobre las características de los servicios a prestar.

Las principales funciones, dentro de su ámbito de actuación, son las siguientes:

a) Ayudar a determinar los requisitos de seguridad de los servicios a prestar, categorizando los servicios mediante la valoración de los impactos de los incidentes que puedan producirse.

b) Proporcionar la información necesaria a la Unidad de Seguridad TIC para realizar los preceptivos análisis de riesgos, con la finalidad de establecer las salvaguardas a implantar. Para ello contará con la ayuda de los responsables de la Información y de los responsables de los Sistemas.

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

10. Responsable de los Sistemas.

El responsable de todos los Sistemas del SAE será la persona titular de la Jefatura del Servicio de informática y figurarán en la documentación de seguridad de los sistemas de información. Para cada sistema de información deberá existir una persona Responsable de Sistema, siendo posible que una misma persona sea responsable de varios sistemas.

Sus principales responsabilidades serán:

a) Supervisar el desarrollo, operación y mantenimiento de los sistemas de información durante todo su ciclo de vida, así como las especificaciones de los mismos, la instalación y verificación de su correcto funcionamiento.

b) Ser la primera persona responsable de la seguridad de los sistemas de información que dirija, velando porque la seguridad TIC esté presente en todas y cada una de las partes de sus ciclos de vida. Especialmente deberá velar porque el desarrollo de los sistemas siga las directrices de seguridad establecidas de manera horizontal por la Junta de Andalucía de acuerdo con los criterios y requisitos técnicos de seguridad aplicables definidos por la Unidad de Seguridad TIC del SAE.

c) Creación, mantenimiento y actualización continua de la documentación de seguridad de los sistemas de información, con el asesoramiento de la Unidad de Seguridad TIC.

d) Asesorar en la definición de la tipología y sistema de gestión de los sistemas de información estableciendo los criterios de uso y los servicios disponibles en el mismo.

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

00253156

f) Cerciorarse de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad.

g) Asesorar en colaboración con la Unidad de Seguridad TIC, a los responsables de la Información y a los responsables de los Servicios, en el proceso de la gestión de riesgos.

h) Suspender el manejo de una cierta 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 debe ser acordada con las personas responsables de la Información afectada, del Servicio afectado y con la Unidad de Seguridad TIC, antes de ser ejecutada.

11. Resolución de conflictos.

Los conflictos entre las diferentes personas, unidades u órganos responsables que componen la estructura organizativa de la política de seguridad TIC serán resueltos por el superior jerárquico común. En su defecto, prevalecerá la decisión del Comité de 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 la normativa de protección de datos de carácter personal prevalecerá la decisión que presente un mayor nivel de exigencia respecto a la protección de los datos de carácter personal.

12. Obligaciones del personal.

Todo el personal que preste servicios en el SAE tiene la obligación de conocer y cumplir la política de seguridad TIC y la normativa de seguridad derivada, siendo responsabilidad del Comité de Seguridad TIC disponer los medios necesarios para que la información llegue a las personas afectadas.

Todo el personal que se incorpore a la Agencia o vaya a tener acceso a alguno de sus sistemas de información o la información gestionada por ellos deberá ser informado de la política de seguridad TIC.

Procederá el ejercicio de las acciones pertinentes para la exigencia de las responsabilidades legales que correspondan por el incumplimiento manifiesto de la política de seguridad TIC o de la normativa de seguridad derivada.

El personal del SAE deberá cumplir además con las instrucciones y normas que regulen el comportamiento del personal empleado público en el uso de los sistemas informáticos y redes de comunicaciones de la Administración de la Junta de Andalucía.

Cualquier persona que actúe bajo la autoridad del Responsable o del Encargado de un Tratamiento de datos personales en el ámbito de aplicación de este documento y tenga acceso a datos personales solo tratará dichos datos siguiendo instrucciones del Responsable, salvo que se lo impida el ordenamiento jurídico comunitario, nacional o autonómico.

13. Desarrollo.

Las medidas sobre la seguridad TIC, de obligado cumplimiento, se desarrollarán en distintos niveles con diferente ámbito de aplicación, detalle técnico y obligatoriedad de cumplimiento, pero de manera que cada elemento de desarrollo se fundamente en el nivel superior.

Dichas medidas conformarán el Marco Normativo de Seguridad de los Sistemas de Información del SAE. Además, se observará lo establecido en la disposición adicional primera 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.

00253156

Todos estos niveles prestarán especial atención a las exigencias derivadas del Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, así como a la normativa aplicable en materia de protección de datos de carácter personal.

Los niveles de desarrollo son los siguientes:

a) Primer nivel: Política de seguridad TIC, constituido por el presente documento. Es de obligado cumplimiento en toda el SAE.

b) Segundo nivel: Normas de seguridad. Son de obligado cumplimiento en todo el SAE y deben ser aprobadas por el Comité de Seguridad TIC. Describen de forma general los principios y normas de seguridad que serán concretados en los niveles posteriores.

c) Tercer nivel: Procedimientos. Describen las acciones a realizar, de una manera más específica, en un proceso relacionado con la seguridad. Son dependientes de las normas de seguridad. Los aprueba el responsable de Sistemas.

d) Cuarto nivel: Documentación técnica. En este último nivel se puede incluir todo tipo de documentación técnica o especializada que se considere necesario para completar y facilitar el desarrollo de las medidas de seguridad. La aprueba el Responsable de Sistemas.

El Comité de Seguridad TIC establecerá los mecanismos necesarios para compartir la documentación derivada del desarrollo con el propósito de regularizarlo, en la medida de lo posible, en todo el ámbito de aplicación de la política de seguridad TIC.

La siguiente tabla resume el marco de desarrollo y la competencia para su aprobación:

Nivel	Documento	Aprueba
Primero	Política de seguridad	Presidencia SAE.
Segundo	Normas de seguridad	Comité de Seguridad TIC.
Tercero	Procedimientos	Responsable de Sistemas.
Cuarto	Documentación técnica	Responsable del Sistemas.

La Unidad de Seguridad TIC se encarga de la gestión de los documentos indicados, debiendo asegurar que ésta sea completa y proporcione información suficiente para definir las necesidades de protección de la información y los activos asociados a la misma en el ámbito de la Agencia.

14. Gestión de riesgos.

La gestión de riesgos deberá realizarse de manera continua sobre el sistema de información, conforme a los principios de gestión de la seguridad basada en los riesgos y con reevaluación periódica de los mismos.

Las personas encargadas de la categorización de los sistemas serán los Responsables de la Información y de los Servicios, siendo la Unidad de Seguridad TIC la encargada de supervisar los análisis de riesgos y proponer las medidas de seguridad a aplicar.

Al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos de carácter personal, en particular como consecuencia de la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, así como la comunicación o acceso no autorizados a dichos datos.

Los Responsables de la Información y de los Servicios son los responsables de aceptar los riesgos residuales calculados en el análisis sobre la información y los servicios, respectivamente, y de realizar su seguimiento y control, sin perjuicio de la posibilidad de delegar esta tarea.

El proceso de gestión de riesgos, que comprende las fases de categorización de los sistemas, análisis de riesgos y selección de medidas de seguridad a aplicar, que deberán ser proporcionales a los riesgos y estar justificadas, deberá revisarse al menos

00253156

con periodicidad anual por parte de la Unidad de Seguridad TIC, que elevará un informe al Comité de Seguridad TIC.

15. Clasificación y control de activos.

Los recursos informáticos y la información del SAE se encontrarán inventariados, con una persona responsable asociada y, en caso de ser necesario, una persona custodia de los mismos. Los inventarios se mantendrán actualizados para asegurar su validez.

Los activos de información estarán clasificados de acuerdo con su sensibilidad y criticidad para el desarrollo de la actividad del SAE, en función de la cual se establecerán las medidas de seguridad exigidas para su protección.

16. Auditorías de la seguridad.

Los sistemas de información serán objeto de una auditoría regular ordinaria, al menos cada dos años, que verifique el cumplimiento de los requerimientos del ENS. Estas auditorías ordinarias, así como las extraordinarias se harán de acuerdo con lo establecido en el art. 34 del Real Decreto 3/2010, de 8 de enero, y la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información, aprobada por Resolución de 27 de marzo de 2018, de la Secretaría de Estado de Función Pública.

Los informes de auditoría serán presentados a la persona Responsable del Sistema competente, al Delegado de Protección de Datos, si afectara a estos, y a la persona responsable de la Unidad de Seguridad TIC. Estos informes serán analizados por esta última persona que presentará sus conclusiones a la persona Responsable del Sistema para que adopte las medidas correctoras adecuadas. Los resultados obtenidos determinarán las líneas de actuación a seguir y las posibles modificaciones a realizar sobre los controles y la normativa de seguridad.

Con el fin de optimizar la utilización de los recursos públicos y garantizar una mejor coordinación entre seguridad TIC y seguridad de protección de datos, siempre que sea posible, las auditorías de seguridad de sistemas de información y las auditorías de protección de datos o medidas análogas de verificación, evaluación y valoración de seguridad de los tratamientos se realizarán de manera conjunta.

17. Protección de datos de carácter personal.

17.1. Incidencia de la normativa de protección de datos de carácter personal.

Todos los sistemas de información del SAE se ajustarán a lo exigido por el Reglamento 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, por el que se aprueba el Reglamento General de Protección de Datos (en adelante, RGPD); la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPDGDD), que adapta el ordenamiento jurídico español al RGPD y completa y desarrolla sus disposiciones, así como el resto de la normativa general o sectorial de protección de datos de carácter personal que sea de aplicación. Todos los tratamientos de datos de carácter personal, automatizados o no automatizados, se sujetarán a la citada norma cuando se encuentren dentro de su ámbito de aplicación.

En dicho ámbito cada Responsable del Tratamiento de datos de carácter personal aplicará las medidas técnicas y organizativas apropiadas a fin de garantizar y ser capaz de demostrar que los tratamientos de datos de carácter personal son conformes con dicha normativa, de acuerdo con el principio de responsabilidad proactiva, de conformidad con el artículo 24 del RGPD. En caso de conflicto con la normativa de seguridad prevalecerá el criterio que presente un mayor nivel de exigencia respecto a la protección de los datos de carácter personal.

Teniendo en cuenta el estado de la técnica, los costes de aplicación y la naturaleza, el alcance, el contexto y los fines del tratamiento de datos de carácter personal, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de

00253156

las personas físicas, y de conformidad con el artículo 32 del RGPD, el Responsable y el Encargado del Tratamiento en el ámbito de aplicación de este documento, aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:

a) La seudonimización y el cifrado de datos personales.

b) La capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.

c) La capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico.

d) Un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

Cuando sea probable que un tipo de tratamiento de datos personal, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, el Responsable del Tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales, de conformidad con el artículo 32 del RGPD. Una única evaluación podrá abordar una serie de operaciones de tratamiento similares que entrañen altos riesgos similares. Para ello recabará el asesoramiento del Delegado de Protección de Datos.

El Responsable del Tratamiento llevará un registro de las actividades de tratamiento de datos de carácter personal efectuadas bajo su responsabilidad, de acuerdo con lo establecido en el artículo 35 del RGPD y el resto de normativa de datos de carácter personal aplicable. Cada Encargado del Tratamiento llevará un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta de un Responsable, de acuerdo con el mismo precepto.

En caso de violación de la seguridad de los datos personales, el Responsable del Tratamiento la notificará a la autoridad de control competente sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas. Si la notificación a la autoridad de control no tiene lugar en el plazo de 72 horas, deberá ir acompañada de indicación de los motivos de la dilación. Cuando sea probable que la violación de la seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas, el Responsable del Tratamiento la comunicará al interesado sin dilación indebida. Dicha notificación y comunicación se atendrán a lo establecido en los artículos 33 y 34 del RGPD y el resto de normativa de datos de carácter personal aplicable.

17.2. Responsables de los Tratamientos de datos de carácter personal.

Los Responsables de los Tratamientos de datos de carácter personal en el ámbito de aplicación de esta Orden son las autoridades públicas que determinen los fines y medios de los tratamientos, de conformidad con el artículo 4.7 del RGPD.

En el ámbito de la política de seguridad TIC del SAE, los Responsables de la Información, es decir, los órganos directivos, tendrán la condición de Responsables del Tratamiento respecto a los tratamientos sobre los que determinen sus fines y medios, salvo que las normas aplicables sobre asignación de atribuciones en materia de protección de datos de carácter personal dispongan otra cosa.

17.3. Encargados de los Tratamientos de datos de carácter personal.

Si los Responsables de los Tratamientos designaran a un Encargado del Tratamiento lo harán únicamente por cada tratamiento a un Encargado de Tratamiento que ofrezca garantías suficientes para aplicar las medidas técnicas y organizativas apropiadas para que el tratamiento sea conforme al RGPD y garantice la protección de los derechos de las personas interesadas, de conformidad con el artículo 28 del RGPD.

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

00253156

Tanto el Responsable como el Encargado del Tratamiento deberá determinar claramente cuándo el tratamiento se realiza bajo su autoridad, conforme a lo establecido en el artículo 29 del RGPD y cuándo se realiza mediante un Encargado de Tratamiento sujeto a lo establecido en el artículo 28 de dicho RGPD.

17.4. Delegado de Protección de Datos.

Existirá una persona que ostente la condición de Delegado de Protección de Datos a efectos de lo establecido en los artículos 37 y 38 del RGPD, para varios de los órganos y unidades administrativas del Servicio Andaluz de Empleo que formen parte de Administración de la Junta de Andalucía, de conformidad con la posibilidad establecida en el artículo 37.3 de dicho Reglamento.

La persona que ostente la condición de Delegado de Protección de Datos será designada por la persona titular de la Dirección Gerencia entre personal adscrito a la Agencia, no pudiendo ser removida ni sancionada por desempeñar sus funciones, salvo que incurriera en dolo o negligencia grave en su ejercicio. La resolución por la que se le designe determinará los órganos o unidades administrativas centrales o periféricos que dependan funcionalmente del SAE o estén adscritos respecto a los que ejercerá sus funciones.

La persona que ostente la condición de Delegado de Protección de Datos podrá poner en conocimiento del Comité de Seguridad TIC las cuestiones relacionadas con la protección de datos que sea necesario y participará, desde el inicio, en todas las cuestiones relacionadas con la protección de datos, contribuyendo así al cumplimiento de la protección de datos personales desde el diseño y por defecto.

Son funciones de la persona que ostente la condición de Delegado de Protección de Datos, entre las demás que le corresponden de conformidad con el artículo 39 del RGPD y demás normativa de aplicación, las siguientes:

a) Ser consultado sobre la contratación, análisis, diseño, operación y mantenimiento de los tratamientos realizados sobre datos personales. También debe ser consultado sobre todo proyecto normativo que suponga un tratamiento de datos personales.

b) Asesorar sobre la confección de los modelos de formularios de recogida de datos personales.

c) Asesorar sobre la evaluación de impacto relativa a la protección de datos, tanto en la necesidad de su realización como en su elaboración.

d) Supervisar la gestión del registro de actividades de tratamiento de los Responsables de Tratamiento del SAE, debiendo éstos facilitarle la nformación necesaria para ello.

e) Asesorar al Responsable del Tratamiento sobre la oportunidad y modo de notificar los incidentes de seguridad sobre datos de carácter personal a la autoridad de control correspondiente en materia de protección de datos de carácter personal.

f) Asesorar al Responsable del Tratamiento sobre la oportunidad y modo de informar a las personas interesadas y afectadas por violaciones de la seguridad de sus datos personales que entrañen un alto riesgo para los derechos y libertades de las personas físicas, conforme a lo establecido en el artículo 34 del RGPD.

18. Formación y concienciación en seguridad TIC.

Anualmente se desarrollarán actividades de formación y concienciación en seguridad TIC destinadas a las personas empleadas públicas del SAE. Entre tales actividades se incluirán las de difusión de esta política de seguridad TIC y de su desarrollo normativo.

A N E X O

REQUISITOS MÍNIMOS

Para la correcta implementación y cumplimiento de la presente Política de Seguridad es necesario aplicar una serie de requisitos de obligatorio cumplimiento.

00253156

1. La seguridad en la organización.

La seguridad debe comprometer a todas las personas integrantes del SAE, sin excepción.

En el apartado 3 de la Política de Seguridad TIC SAE«Organización y gestión de la seguridad TIC», se especifica la organización de la seguridad con la definición de la estructura organizativa. Asimismo, la implementación de dicha organización está en el marco normativo cubierto por el establecimiento de un Sistema de Gestión de la Seguridad, basado en el ENS.

2. Análisis y gestión de riesgos.

Los servicios e infraestructuras bajo el alcance de la presente Política de Seguridad deberán estar sometidos a un análisis de riesgos para orientar las medidas de protección a minimizar los mismos como se indica en el apartado 14 «Gestión de riesgos»

La descripción de la metodología y evaluación del riesgo seguidas están desarrolladas en «Metodología de análisis y gestión de riesgos».

El análisis de riesgos se realizará igualmente cuando se vaya a iniciar o a modificar un tratamiento de datos de carácter personal, en línea a lo establecido en el RGPD y la LOPDGDD.

En estos casos se contemplarán en el alcance del análisis todos aquellos activos que intervengan en el tratamiento, considerando tanto activos relacionados con los sistemas de información, como humanos, locales o terceros.

A raíz de los resultados obtenidos en los mencionados análisis de riesgos se determinarán las medidas necesarias para proteger dichos datos.

3. Gestión de personal.

En el apartado 12 «Obligaciones del personal» de la presente Política de Seguridad, en las normativas de uso internos correspondientes se detallan la obligatoriedad de conocimiento y concienciación en materia de seguridad según sus responsabilidades. Los recursos necesarios para la implantación del sistema de seguridad, así como aquellos que lleven a cabo su operación, mantenimiento, supervisión, o tenga relación con el sistema, se establecerá en el marco normativo de la Política de Seguridad TIC del SAE, y será aprobados por parte del órgano competente del organismo a propuesta del Comité de Seguridad TIC.

La selección de personal se llevará a cabo aplicando los criterios por parte del Servicio de Personal del SAE.

4. Profesionalidad.

Siguiendo lo indicado en el apartado 19 «Formación y concienciación en Seguridad TIC» de la presente Política de Seguridad, se desarrollan los objetivos de las acciones de formación y concienciación y en los apartados 4.1 «Funciones del Comité de Seguridad TIC», 6 «Unidad de Seguridad TIC» , 7 «Responsable de Seguridad TIC» , 8 «Responsables de la Información», 9 «Responsables de los Servicios», 10 «Responsables de los Sistemas», 12 «Obligaciones del personal» de la presente Política de Seguridad y en la normativa de uso interno correspondiente se indican las responsabilidades del personal.

Con periodicidad anual se diseñará un plan de formación específico en el que se tendrá en cuenta las necesidades de profesionalidad del sistema de seguridad.

5. Autorización y control de acceso.

El acceso a los sistemas de información estará restringido y limitado a aquellas personas usuarias o procesos que lo necesiten para el desarrollo de su actividad y estén previamente autorizados.

00253156

El acceso a la información seguirá el principio de «necesidad de conocer», de forma que los privilegios otorgados a cada entidad sean los mínimos imprescindibles para el desarrollo de su actividad.

La identificación de las personas usuarias será tal que se pueda conocer en todo momento quién recibe los derechos de acceso y quién ha realizado alguna actividad, por lo que los identificadores serán personales, no compartidos e intransferibles.

Los lugares con acceso restringido igualmente se controlarán y serán previamente autorizados por los responsables asignados.

6. Protección de las instalaciones.

Los sistemas de información estarán ubicados en zonas protegidas, con acceso restringido, habilitado únicamente al personal autorizado.

7. Adquisición de productos.

Para las actividades de adquisición de nuevos productos, sistemas o servicios se establecen actuaciones de análisis de riesgos con proveedores y se mantendrán actualizados los listados de proveedores habituales. Las adquisiciones se autorizarán por los responsables del área implicada y el Servicio de Contratación a través de informes favorables del proveedor, en caso de requerirse.

8. Seguridad por defecto.

Los sistemas y aplicaciones se diseñarán y construirán bajo el principio de seguridad por defecto, de tal forma que:

a) El sistema ofrecerá la funcionalidad mínima necesaria y ninguna adicional. Cualquier función que no sea de interés o innecesaria será deshabilitada o no implantada.

b) La operación y explotación de los sistemas estará limitada a aquellas personas o ubicaciones que se autoricen, quedando prohibidas para el resto.

c) El uso del sistema ha de ser seguro, de tal forma que el uso inseguro requerirá intención expresa por parte del usuario.

La seguridad estará presente desde la concepción de un sistema o aplicación y permanecerá presente durante todo su ciclo de vida.

En la concepción de un nuevo sistema o aplicación, o modificación sustancial de un sistema o aplicación existentes, se contará siempre, y desde el inicio, con la participación del Responsable de Seguridad de la Información.

9. Integridad y actualización del sistema.

Se deberán seguir en todo momento las informaciones acerca de la vulnerabilidades que afectan a los sistemas de información.

Se seguirán las recomendaciones de los fabricantes de equipos y software en cuanto a actualizaciones de seguridad, que deberán ser analizadas en cuanto a su idoneidad y conveniencia, y aplicadas en caso positivo con la menor dilación.

10. Protección de la información almacenada y en tránsito.

Se protegerán los entornos que contienen información almacenada y en tránsito entre entornos inseguros. En este sentido se protegerán convenientemente los equipos portátiles que puedan contener información, así como los soportes extraíbles (lápices de memoria, discos duros extraíbles, etc.).

11. Prevención ante otros sistemas de información interconectados.

Se desplegarán las protecciones necesarias para proteger el perímetro de la red corporativa del SAE, de forma que se neutralicen las posibles intrusiones procedentes del exterior, ya sea iniciadas malintencionadamente por terceros o como consecuencia de la interconexión con sistemas de terceros.

00253156

12. Registros de actividad.

Los sistemas y aplicaciones generarán los registros de actividad necesarios para conocer su actividad, de forma que se pueda determinar en todo momento qué persona actúa, sobre qué datos, con qué operaciones y sus privilegios de acceso.

13. Gestión de incidentes de seguridad.

El SAE definirá e implantará procedimientos de gestión de incidencias de seguridad que aseguren la correcta gestión y respuesta efectiva que permita anular o minimizar el impacto del incidente en la información, los servicios, los empleados, las personas usuarias y, en general, en la actividad del SAE.

El procedimiento de gestión y respuesta a incidentes de seguridad contemplará la comunicación y notificación de los incidentes a los organismos receptores de dicha información de acuerdo con la legalidad vigente.

14. Continuidad de negocio.

Para asegurar la disponibilidad de los servicios y sistemas de información, el SA diseñará e implantará Planes de Continuidad de servicio que eviten las interrupciones de las actividades del SAE y garanticen, ante una contingencia, la reanudación de los servicios y sistemas de información a los niveles adecuados de operatividad.

15. Gestión de la seguridad y mejora continua.

Se deberá establecer un Sistema de Gestión de la seguridad que permita conocer en cada memento el estado de la seguridad, mediante la definición y medida de indicadores, y permita tomar las decisiones informadas pertinentes para cumplir los requisitos de seguridad establecidos.

Se establecerá un proceso de mejora continua mediante el análisis de la situación, la implantación de nuevas medidas de seguridad, la mejora de las existentes y la aportación de mejoras sugeridas por el Comité de Seguridad TIC y por todo el SAE en su conjunto.

00253156