MINISTERIO
DE AGRICULTURA, PESCA
Y ALIMENTACIÓN

Resolución de 16 de febrero de 2026 de la Directora de la Agencia de Información y Control Alimentarios, O.A, por la que se aprueba la Política se Seguridad de la Información del organismo y se crea el Comité de Seguridad de la Información.

La relación con la ciudadanía, las empresas y las entidades del sector público a través de la Administración digital necesita de la plena confianza en la seguridad de la información, tal y como se establece en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, que, en su artículo 13, dispone los derechos de las personas en sus relaciones con las Administraciones Públicas, incluyendo en su apartado h) el derecho a la protección de datos de carácter personal y, en particular, a la seguridad y confidencialidad de los datos que figuren en los ficheros, sistemas y aplicaciones de las Administraciones Públicas.

Por otra parte, la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, es la que establece, en su artículo 3, la necesidad de que las Administraciones Públicas se relacionen entre sí y con sus órganos, organismos públicos y entidades vinculadas o dependientes a través de medios electrónicos que garanticen la interoperabilidad y seguridad de los sistemas y soluciones adoptadas por cada una de ellas; y faciliten la prestación de servicios a los interesados preferentemente por dichos medios, consagrando, en su artículo 156, al Esquema Nacional de Seguridad como instrumento fundamental para el logro de dichos objetivos. Este Esquema establece la política de seguridad en la utilización de medios electrónicos, así como los principios básicos y requisitos mínimos que garanticen adecuadamente la seguridad de la información tratada.

El Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, persigue alcanzar una protección adecuada de la información y de los servicios prestados por las entidades de su ámbito de aplicación, con objeto de garantizar el acceso, la confidencialidad, la integridad, la trazabilidad, la autenticidad, la disponibilidad y la conservación de los datos y los servicios utilizados por medios electrónicos en el ejercicio de sus competencias.

En el ámbito de la Agencia de Información y Control Alimentarios, O.A, (en adelante, AICA), de acuerdo con lo que prevé el Esquema Nacional de Seguridad, se deberá garantizar la seguridad como un proceso integral constituido por todos los recursos humanos, materiales, técnicos, jurídicos y organizativos relacionados con los sistemas de información que deberán estar preparados para prevenir, detectar, reaccionar y recuperarse de incidentes, garantizando la conservación de los datos e información en soporte electrónico.

La Política de Seguridad de la Información de AICA, tal y como dispone el apartado 3.1. del anexo II del Real Decreto 311/2022, de 3 de mayo, constituye la medida fundamental del marco organizativo y de la estructura normativa en materia de seguridad de la información. Así mismo, en el artículo 12, se establece que esta política debe considerar los riesgos que se derivan del tratamiento de los datos personales, para lo cual se ha tenido en cuenta la normativa de protección de datos, en particular la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, y el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo 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.

Por tanto, en el ejercicio de las competencias que tiene atribuidas, esta Dirección ha resuelto:

PRIMERO. Misión y objetivos.

AICA es un organismo autónomo, adscrito al Ministerio de Agricultura, Pesca y Alimentación, a través de la Secretaría General de Recursos Agrarios y Seguridad Alimentaria, creado mediante la Ley 12/2013, de 2 de agosto, de medidas para mejorar el funcionamiento de la cadena alimentaria, que tiene como finalidad controlar los derechos y obligaciones establecidos en dicha ley, instruyendo o iniciando el procedimiento sancionador si detecta infracciones a la misma.

A continuación, se resumen las principales competencias de AICA:

1.En materia de control de la Ley 12/2013, de 2 de agosto:

a) Establecer y desarrollar, en el ámbito de las competencias de la Administración General del Estado, el régimen de control necesario para comprobar el cumplimiento de la Ley 12/2013, de 2 de agosto,

b) Realizar las comprobaciones que corresponda de las denuncias por incumplimientos de lo dispuesto en la Ley 12/2013, de 2 de agosto, que sean presentadas ante AICA.

c) Iniciar de oficio el procedimiento sancionador que corresponda por las irregularidades que constate en el ejercicio de sus funciones que supongan incumplimientos de la Ley 12/2013, de 2 de agosto y, tras la correspondiente instrucción, proponer a la autoridad competente la resolución que proceda o, en su caso, formular denuncia ante la Comisión Nacional de los Mercados y de la Competencia, debidamente documentada.

d) Gestionar el registro digital regulado en el artículo 11.bis de la Ley 12/2013, de 2 de agosto, en el que se inscribirán los contratos alimentarios y sus modificaciones suscritos con los productores primarios y sus agrupaciones.

2. En materia de sistemas de información:

a) Gestionar y mantener los sistemas de información en los sectores oleícolas (aceites de oliva y aceitunas de mesa), lácteos y vinícolas.

b) Establecer y desarrollar el régimen de control necesario para comprobar el cumplimiento de las obligaciones por parte de los operadores de los sectores oleícolas y que le hayan sido encomendadas por las comunidades autónomas a través de encomiendas de gestión.

c) Coordinar con las comunidades autónomas los Planes de Control dirigidos a verificar la veracidad de los datos incorporados al sistema de información procedentes de las declaraciones efectuadas por los operadores del sector oleícola, vinícola y lácteo (SIMO, INFOVI e INFOLAC).

3. En materia de Organizaciones Interprofesionales:

a) Iniciar e instruir el procedimiento sancionador derivado de las denuncias presentadas por las organizaciones interprofesionales por incumplimiento de los pagos de las aportaciones obligatorias establecidas en la extensión de norma (aceite de oliva, aceituna de mesa, orujo, lácteo, vino).

SEGUNDO. Marco normativo.

La normativa de referencia en esta materia será:

a) Ley 12/2013, de 2 de agosto.

C/ INFANTA MERCEDES, 31.
4ª planta
28020 MADRID
Teléfono: 91 347 8369

b) Real Decreto 227/2014, de 4 de abril, por el que se aprueba el Estatuto de la Agencia de Información y Control Alimentarios.

c) Real Decreto 66/2015, de 6 de febrero, por el que se regula el régimen de controles a aplicar por la Agencia de Información y Control Alimentarios, previstos en la Ley 12/2013, de 2 de agosto, de medidas para mejorar el funcionamiento de la cadena alimentaria.

d) Real Decreto 64/2015, de 6 de febrero, por el que se desarrolla parcialmente la Ley 12/2013, de 2 de agosto, de medidas para mejorar el funcionamiento de la cadena alimentaria, y se modifica el Reglamento de la Ley 38/1994, de 30 de diciembre, reguladora de las organizaciones interprofesionales agroalimentarias, aprobado por Real Decreto 705/1997, de 16 de mayo.

e) Real Decreto 1028/2022, de 20 de diciembre, por el que se desarrolla el Registro de Contratos Alimentarios.

f) Ley 40/2015, de 1 de octubre, Régimen Jurídico del Sector Publico

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

h) Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE.

i) Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

TERCERO. Objetivo y alcance.

1. El propósito de esta resolución es definir y aprobar la Política de Seguridad de la Información de AICA, la cual debe recoger el conjunto de directrices que rigen la forma en que una organización gestiona y protege la información que trata y los servicios que presta.

2.La Política de Seguridad de la Información será de obligado cumplimiento para todo el personal de AICA, que acceda tanto a los sistemas de información como a la propia información que sea gestionada por el organismo, con independencia de cuál sea su destino, adscripción o relación con el mismo.

CUARTO. Principios básicos.

La Política de Seguridad de la Información se desarrollará con carácter general de acuerdo con los siguientes principios:

1. Principio de confidencialidad: se deberá garantizar que los activos sean accesibles únicamente para aquellas personas expresamente autorizadas para ello.

2. Principio de integridad y actualización del sistema: se deberá asegurar que la información con la que se trabaja sea completa y precisa, y se incidirá en la exactitud tanto de su contenido como de los procesos involucrados.

3. Principio de disponibilidad, resiliencia y continuidad: se garantizará la prestación continuada de los servicios y la recuperación inmediata ante posibles contingencias, mediante medidas de recuperación orientadas a la restauración de los servicios y de la información asociada. Se debe procurar que los activos estén disponibles cuando lo requieran las personas autorizadas para acceder a ellos.

4. Principio de autenticidad: se deberá garantizar que la información se intercambie con los interlocutores idóneos y que los servicios se acrediten correctamente.

5. Principio de trazabilidad: se deberá garantizar el seguimiento de las operaciones efectuadas sobre la información y los servicios que lo requieran, registrándose la actividad de los usuarios.

6. Principio de seguridad integral: la seguridad será considerada como parte de la operativa habitual y como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos relacionados con el sistema, evitando, salvo casos de urgencia o necesidad, cualquier actuación puntual o tratamiento coyuntural. Además, estará presente y aplicándose desde el diseño inicial de los sistemas de información.

7. Principio de gestión del riesgo: gestionar la seguridad de la información consiste en analizar los riesgos, establecer medidas de seguridad adecuadas, eficaces y proporcionadas e incluir la corrección y mejora continuas que lleven a que la organización sea cada vez más preventiva que reactiva frente a los incidentes de seguridad. Se deberán minimizar los riesgos hasta niveles aceptables y buscar el equilibrio entre las medidas de seguridad y la naturaleza de la información.

8. Principio de prevención, reacción, recuperación y conservación: se desarrollarán planes y líneas de trabajo específicas orientadas a la prevención, detección, corrección de fraudes, incumplimientos o incidentes relacionados con la seguridad, así como de protección de las instalaciones del organismo y a la plataforma tecnológica comprendida en el alcance.

Asimismo, se mantendrán disponibles los servicios durante todo el ciclo de vida de la información digital, a través de los procedimientos necesarios para la preservación del patrimonio digital del organismo, garantizando la conservación de los datos e información en soporte electrónico.

9. Principio de mejora y reevaluación continua: se revisará, de manera recurrente, el grado de eficacia de los controles de seguridad implantados en la organización para aumentar la capacidad de adaptación a la constante evolución de los riesgos y del entorno tecnológico.

10. Principio de proporcionalidad en coste: la implantación de medidas que mitiguen los riesgos de seguridad de los activos deberá hacerse dentro del marco presupuestario previsto a tal efecto y siempre buscando el equilibrio entre las medidas de seguridad, la naturaleza de la información y el presupuesto previsto.

11. Principio de concienciación y formación: se articularán programas de formación, sensibilización y concienciación para las personas usuarias en materia de seguridad de la información, debidamente apoyados en las políticas corporativas y con un acomodado proceso de seguimiento y actualización.

QUINTO. Estructura de la seguridad.

La estructura de la seguridad de AICA se establecerá en tres niveles:

1. Nivel de Gobierno: que entiende la misión de la organización, determina los objetivos que se propone alcanzar y responde de que se alcancen.

Estará representado por el Comité de Seguridad de la Información (en adelante, CSEG).

2. Nivel de Supervisión: que entiende qué hace cada departamento y cómo se coordinan entre sí para alcanzar los objetivos marcados por la Dirección.

Estará representado por la Secretaría General de AICA.

3. Nivel de Operación: que se centra en una actividad concreta y controla cómo se hacen las cosas.

Estará representado por la Jefatura del Servicio de Informática.

Dicha estructura, en el ámbito descrito por la Política de seguridad de la Información de AICA, estará compuesta por los siguientes roles:

a) El Comité de Seguridad de la Información (CSEG).

b) El Responsable de la Información (RINF).

c) El Responsable del Servicio (RSERV).

d) El Responsable de Seguridad (RSEG).

e) El Responsable del Sistema (RSIS).

f) El Delegado de Protección de Datos (DPD).

Salvo la figura del Delegado de Protección de Datos (DPD) cuya responsabilidad está transferida al departamento ministerial al cual está adscrita AICA, el resto de los roles individuales estarán asignados de la siguiente manera:

Figura/Cargo	**Nivel**	**Responsabilidad**
Comité de Seguridad de la Información	Gobierno	– Responsable de la Información (RINFO) – Responsable del Servicio (RSERV)
Titular de la Secretaría General	Supervisión	– Responsable de Seguridad (RSEG)
Titular de la Jefatura de Servicio de Informática	Operación	– Responsable del Sistema (RSIS)

Los roles de seguridad serán revisados cada dos años. En el caso de que se produzca una vacante, la misma deberá ser cubierta en el plazo de un mes.

SEXTO. El Comité de Seguridad de la Información.

1. Se crea el CSEG, adscrito a la Dirección de AICA.

El CSEG estará compuesto por los siguientes miembros:

Miembro	**Cargo**
Presidente/a	– Titular de la Secretaría General de AICA
Vicepresidente/a	– Coordinador/a del Área de Tramitación y Relaciones con Juzgados.

C/ INFANTA MERCEDES, 31.
4ª planta
28020 MADRID
Teléfono: 91 347 8369

Vocales	– Titular de la Jefatura de Servicio de Informática. – Titular de la Unidad de Relaciones Internacionales y Asuntos Horizontales. – Asesor/a jurídico/a de AICA, si existiera ese puesto. – Delegado/a de Protección de Datos del Ministerio de Agricultura, Pesca y Alimentación

2. El CSEG ejercerá las siguientes funciones:

a) Elaborar las propuestas de modificación y actualización permanente que se hagan sobre la Política de Seguridad de la Información.

b) Aprobar el resto de la normativa de seguridad de primer nivel definida en esta resolución.

c) Velar e impulsar el cumplimiento de la Política y su desarrollo.

d) Promover la mejora continua en la gestión de la seguridad de la información.

e) Aprobar el Plan de Auditoría y el Plan de Formación propuestos por el Responsable de Seguridad.

f) Resolver los posibles conflictos que puedan derivarse del establecimiento de la citada estructura organizativa.

g) Elaborar estudios, análisis previos y propuestas de modificación y actualización de la política.

h) Elaborar estudios, análisis previos y propuestas sobre la normativa de seguridad de segundo y tercer nivel definida en esta resolución.

i) Analizar el cumplimiento de la Política.

j) Analizar las medidas de seguridad de la información y de los servicios electrónicos prestados por los sistemas de información.

k) Estudiar las actividades de concienciación y formación en materia de seguridad.

l) Coordinar la comunicación con el Centro Criptológico Nacional en la utilización de servicios de respuesta a incidentes de seguridad.

m) Seguir las medidas de resultado del análisis y gestión de riesgos de los activos.

n) Promover las auditorías internas de seguridad y de conformidad con el Esquema Nacional de Seguridad.

o) Actuar como comité de crisis en caso de incidente de alta o muy alta peligrosidad y/o impacto.

3. El CSEG se reunirá con carácter ordinario, al menos, una vez al año y con carácter extraordinario cuando lo decida su Presidente. De acuerdo con la autorización contenida en el artículo 17 de la Ley 40/2015, de 1 de octubre, se faculta al CSEG para que lleve a cabo las funciones que tiene asignadas por medios electrónicos.

4. El CSEG podrá recabar de personal técnico, propio o externo, la información pertinente para la toma de sus decisiones.

5. Los acuerdos se adoptarán por mayoría de los miembros. En caso de empate, el voto del presidente será dirimente.

C/ INFANTA MERCEDES, 31.
4ª planta
28020 MADRID
Teléfono: 91 347 8369

6. El CSEG se constituirá como el comité de crisis. No será necesaria la totalidad de sus miembros para poder realizar las tareas propias del comité de crisis.

SÉPTIMO. El Responsable de la Información y el Responsable del Servicio.

El Responsable de la Información y el Responsable del Servicio tendrán la potestad, dentro de su ámbito de actuación y de sus competencias, de establecer los requisitos en materia de seguridad de la información que manejan y de los servicios que prestan. Si esta información incluyese datos de carácter personal, además deberán tenerse en cuenta los requisitos derivados de la legislación correspondiente. Dada la estructura de este organismo, éstos dos roles serán desempeñados por la misma persona.

OCTAVO. El Responsable de Seguridad.

1. Conforme al artículo 11 del Real Decreto 311/2022, de 3 de mayo, el Responsable de Seguridad será la persona que determina las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios. Su designación no implica, en ningún caso, aumento de las dotaciones ni las retribuciones de dicho efectivo.

2. Serán funciones del Responsable de Seguridad:

a) Elaborar las propuestas de modificación y actualización permanente que se hagan sobre la Política de la Seguridad de la Información.

b) Elaborar estudios, análisis previos y propuestas de modificación y actualización de la Política.

c) Elaborar estudios, análisis previos y propuestas sobre la normativa de seguridad del segundo y tercer nivel definida en esta resolución.

d) Analizar el cumplimiento de la Política.

e) Analizar las medidas de seguridad de la información y de los servicios electrónicos prestados por los sistemas de información.

f) Estudiar las actividades de concienciación y formación en materia de seguridad.

g) Coordinar la comunicación con el Centro Criptológico Nacional en la utilización de servicios de respuesta a incidentes de seguridad.

h) Seguimiento de las medidas resultado del análisis y gestión de riesgos de los activos.

i) Promover la seguridad de la información manejada y de los servicios electrónicos prestados por los sistemas de información.

j) Elaborar la normativa de seguridad de segundo y tercer nivel definida en esta resolución y velar e impulsar su cumplimiento por parte de los Responsables del Sistema y de cualquier otro agente del sistema.

k) Encargarse de que la documentación de seguridad se mantenga organizada y actualizada, y de gestionar los mecanismos de acceso a la misma.

l) Promover la mejora continua en la gestión de la seguridad de la información.

m) Impulsar la formación y concienciación en materia de seguridad de la información

3. El Responsable de Seguridad podrá recabar de personal técnico, propio o externo, la información pertinente para la toma de sus decisiones.

4. El Responsable de Seguridad podrá convocar el Comité de Crisis en situaciones de emergencia que lo requieran. Este comité estará constituido por los siguientes miembros:

a) El titular de la Dirección de AICA.

b) El titular de la Secretaría General de AICA.

c) Los/las Coordinadores/as de Área.

d) El titular de la Jefatura de Servicio de Informática.

El Comité de Crisis será órgano encargado de gestionar, tomar decisiones y coordinar las acciones necesarias para hacer frente o resolver la emergencia que haya sido calificada como crisis.

NOVENO. El Responsable del Sistema.

1. La designación del Responsable del Sistema no implicará, en ningún caso, aumento de las dotaciones ni las retribuciones de dicho efectivo. Sus funciones serán:

a) Paralizar o dar suspensión al acceso a información o prestación de servicio si tiene el conocimiento de que estos presentan deficiencias graves de seguridad.

b) Desarrollar, operar y mantener el Sistema de Información durante todo su ciclo de vida.

c) Elaborar los procedimientos operativos necesarios.

d) Definir la topología y la gestión del Sistema de Información estableciendo los criterios de uso y los servicios disponibles en el mismo.

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

f) Prestar al Responsable de Seguridad asesoramiento para la determinación de la categoría del Sistema.

g) Colaborar, si así se le requiere, en la elaboración e implantación de los planes de mejora de la seguridad y, llegado el caso, en los planes de continuidad.

h) Llevar a cabo las funciones del administrador de la seguridad del sistema.

i) La gestión, configuración y actualización, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad.

j) La gestión de las autorizaciones concedidas a los usuarios del sistema, en particular los privilegios concedidos, incluyendo la monitorización de la actividad desarrollada en el sistema y su correspondencia con lo autorizado.

k) Aprobar los cambios en la configuración vigente del Sistema de Información.

l) Asegurar que los controles de seguridad establecidos son cumplidos estrictamente.

m) Asegurar que son aplicados los procedimientos aprobados para manejar el Sistema de Información.

n) Supervisar las instalaciones de hardware y software, sus modificaciones y mejoras para asegurar que la seguridad no está comprometida y que en todo momento se ajustan a las autorizaciones pertinentes.

C/ INFANTA MERCEDES, 31.
4ª planta
28020 MADRID
Teléfono: 91 347 8369

o) Monitorizar el estado de seguridad proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica.

DÉCIMO. Desarrollo de la Política de Seguridad de la información.

1. El cumplimiento de los objetivos marcados en esta Política de Seguridad se llevará a cabo mediante el desarrollo de la documentación que componen las normas y procedimientos de seguridad asociados al cumplimiento del Esquema Nacional de Seguridad.

Las normas sobre seguridad de la información serán de obligado cumplimiento y se estructurarán en los siguientes niveles relacionados jerárquicamente:

a) Primer nivel: constituido por la Política de Seguridad de la Información y las directrices generales de seguridad.

b) Segundo nivel: constituido por las normas de seguridad desarrolladas por AICA.

c) Tercer nivel: constituido por los procedimientos, guías e instrucciones técnicas complementarias.

Estos documentos, cumpliendo con lo expuesto en la Política, determinarán las acciones o tareas a realizar en el desempeño de un proceso.

2. El segundo y el tercer nivel deberán:

a) Limitarse única y exclusivamente al ámbito específico de las competencias de AICA. Este ámbito vendrá determinado por los sistemas informáticos y servicios de tecnologías de la información y de las comunicaciones que sean prestados y gestionados directamente por AICA.

b) Cumplir estrictamente con lo indicado en el Esquema Nacional de Seguridad y con el primer y segundo nivel enunciados en el presente apartado.

c) Ser aprobado dentro del ámbito de AICA.

3. Además de los elementos de obligado cumplimiento enunciados en este apartado, se podrá disponer, y siempre dentro del ámbito de sus competencias y responsabilidades, de otros documentos tales como estándares de seguridad, buenas prácticas, informes técnicos, etc.

4. El personal adscrito a la presente Política tendrá la obligación de conocerla y cumplirla, junto con todas las directrices generales, normas y procedimientos de seguridad de la información que puedan afectar a sus funciones.

5. Dichas normas y procedimientos de seguridad estarán a disposición de todo el personal de AICA en su intranet.

UNDÉCIMO. Datos de carácter personal.

AICA cumple, en el tratamiento de los datos personales, con los principios y obligaciones de la normativa vigente, entre otra el Reglamento 679/2016, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, y la Ley Orgánica 3/2018, de 5 de diciembre, respetando, en todo caso, el derecho fundamental a la protección de datos personales, la intimidad y el resto de los derechos fundamentales reconocidos tanto en la legislación y tratados internacionales como en la Constitución vigente.

DUODÉCIMO. Requisitos mínimos.

C/ INFANTA MERCEDES, 31.
4ª planta
28020 MADRID
Teléfono: 91 347 8369

AICA, para lograr el cumplimiento del Real Decreto 311/2022, de 3 de mayo, que recoge los principios básicos y de los requisitos mínimos, implementará diversas medidas de seguridad proporcionales a la naturaleza de la información y los servicios a proteger, teniendo en cuenta la categoría de los sistemas afectados.

1. La seguridad como un proceso integral y mínimo privilegio.

La seguridad se entiende como un proceso integral constituido por todos los elementos técnicos, humanos, materiales, jurídicos y organizativos, relacionados con el sistema. La aplicación del Esquema Nacional de Seguridad a AICA estará presidida por este principio, que excluye cualquier actuación puntual o tratamiento coyuntural.

Se prestará la máxima atención a la concienciación de las personas que intervienen en el proceso y a sus responsables jerárquicos, para evitar que, la ignorancia, la falta de organización y coordinación, o de instrucciones inadecuadas, constituyan fuentes de riesgo para la seguridad.

Los sistemas de información deben diseñarse y configurarse otorgando los mínimos privilegios necesarios para su correcto desempeño, lo que implica incorporar los siguientes aspectos:

a) El sistema proporcionará la funcionalidad imprescindible para que AICA alcance sus objetivos competenciales o contractuales.

b) Las funciones de operación, administración y registro de actividad serán las mínimas necesarias, y se asegurará que sólo son desarrolladas por las personas autorizadas, desde emplazamientos o equipos asimismo autorizados; pudiendo exigirse, en su caso, restricciones de horario y puntos de acceso facultados.

c) En un sistema de explotación se eliminarán o desactivarán, mediante el control de la configuración, las funciones que sean innecesarias o inadecuadas al fin que se persigue. El uso ordinario del sistema ha de ser sencillo y seguro, de forma que una utilización insegura requiera de un acto consciente por parte del usuario.

d) Se aplicarán guías de configuración de seguridad para las diferentes tecnologías, adaptadas a la categorización del sistema, al efecto de eliminar o desactivar las funciones que sean innecesarias o inadecuadas.

2. Vigilancia continua, reevaluación periódica e Integridad, actualización del sistema y mejora continua del proceso de seguridad.

La vigilancia continua por parte de AICA permitirá la detección de actividades o comportamientos anómalos y su oportuna respuesta.

La evaluación permanente del estado de la seguridad de los activos permitirá medir su evolución, detectando vulnerabilidades e identificando deficiencias de configuración.

Las medidas de seguridad se reevaluarán y actualizarán periódicamente, adecuando su eficacia a la evolución de los riesgos y los sistemas de protección, pudiendo llegar a un replanteamiento de la seguridad, si fuese necesario.

La inclusión de cualquier elemento físico o lógico en el catálogo actualizado de activos del sistema, o su modificación, requerirá autorización formal previa.

La evaluación y monitorización permanentes permitirán adecuar el estado de seguridad de los sistemas atendiendo a las deficiencias de configuración, las vulnerabilidades identificadas y las

C/ INFANTA MERCEDES, 31.
4ª planta
28020 MADRID
Teléfono: 91 347 8369

actualizaciones que les afecten, así como la detección temprana de cualquier incidente que tenga lugar sobre los mismos.

El proceso integral de seguridad implantado deberá ser actualizado y mejorado de forma continua. Para ello, se aplicarán los criterios y métodos reconocidos en la práctica nacional e internacional relativos a la gestión de la seguridad de las tecnologías de la información

3. Gestión de personal y profesionalidad

Todo el personal, propio o ajeno relacionado con los sistemas de información de AICA, dentro del ámbito del Esquema Nacional de Seguridad, serán formados e informados de sus deberes, obligaciones y responsabilidades en materia de seguridad. Su actuación será supervisada para verificar que se siguen los procedimientos establecidos.

El significado y alcance del uso seguro del sistema se concretará y plasmará en unas normas de seguridad que serán aprobadas por la Dirección de AICA. De igual modo, se determinarán los requisitos de formación y experiencia necesaria del personal para el desarrollo de su puesto de trabajo.

La seguridad de los sistemas de información estará atendida y será revisada y auditada por personal cualificado, dedicado e instruido en todas las fases de su ciclo de vida: planificación, diseño, adquisición, construcción, despliegue, explotación, mantenimiento, gestión de incidencias y desmantelamiento.

De manera objetiva y no discriminatoria se exigirá que las organizaciones que nos proporcionan servicios cuenten con profesionales cualificados y con unos niveles idóneos de gestión y madurez de los servicios prestados.

4. Gestión de la seguridad basada en los riesgos, análisis y gestión de riesgos

El análisis y la gestión de los riesgos será parte esencial del proceso de seguridad y será una actividad continua y permanentemente actualizada.

La gestión de los riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos a niveles aceptables. La reducción a estos niveles se realizará mediante una apropiada aplicación de medidas de seguridad, de manera equilibrada y proporcionada a la naturaleza de la información tratada, de los servicios a prestar y de los riesgos a los que estén expuestos.

Esta gestión se realizará por medio del análisis y tratamiento de los riesgos a los que está expuesto el sistema. Sin perjuicio de lo dispuesto en el anexo II, se empleará alguna metodología reconocida internacionalmente. Las medidas adoptadas para mitigar o suprimir los riesgos deberán estar justificadas y, en todo caso, existirá una proporcionalidad entre ellas y los riesgos.

5. Incidentes de seguridad, prevención, detección, reacción y recuperación

AICA dispondrá de procedimientos de gestión de incidentes de seguridad de acuerdo con lo previsto en el artículo 33 y en la Instrucción Técnica de Seguridad correspondiente, de mecanismos de detección, criterios de clasificación, procedimientos de análisis y resolución, así como de los cauces de comunicación a las partes interesadas.

La seguridad del sistema contemplará las acciones relativas a los aspectos de prevención, detección y respuesta, al objeto de minimizar sus vulnerabilidades y lograr que las amenazas

C/ INFANTA MERCEDES, 31.
4ª planta
28020 MADRID
Teléfono: 91 347 8369

sobre el mismo no se materialicen o que, en el caso de hacerlo, no afecten gravemente a la información que maneja o a los servicios que presta.

Las medidas de prevención podrán incorporar componentes orientados a la disuasión o a la reducción de la superficie de exposición, deben eliminar o reducir la posibilidad de que las amenazas lleguen a materializarse.

Las medidas de detección irán dirigidas a descubrir la presencia de un ciberincidente.

Las medidas de respuesta se gestionarán en tiempo oportuno, y estarán orientadas a la restauración de la información y de los servicios que pudieran haberse visto afectados por un incidente de seguridad.

El sistema de información garantizará la conservación de los datos e información en soporte electrónico.

De igual modo, el sistema mantendrá disponibles los servicios durante todo el ciclo vital de la información digital, a través de una concepción y procedimientos que sean la base para la preservación del patrimonio digital.

6. Existencia de líneas de defensa y prevención ante otros sistemas de información interconectados

AICA implementará una estrategia de protección del sistema de información constituida por múltiples capas de seguridad, constituidas por medidas organizativas, físicas y lógicas, de tal forma que cuando una capa haya sido comprometida permita desarrollar una reacción adecuada frente a los incidentes que no han podido evitarse, reduciendo la probabilidad de que el sistema sea comprometido en su conjunto y minimizar el impacto final sobre el mismo.

Se protegerá el perímetro del sistema de información, especialmente, cuando el sistema de AICA se conecte a redes públicas, tal y como se definen en la legislación vigente en materia de telecomunicaciones, reforzándose las tareas de prevención, detección y respuesta a incidentes de seguridad.

En todo caso, se analizarán los riesgos derivados de la interconexión del sistema con otros sistemas y se controlará su punto de unión. Para la adecuada interconexión entre sistemas se estará a lo dispuesto en la Instrucción Técnica de Seguridad correspondiente.

7. Diferenciación de responsabilidades, organización e implantación del proceso de seguridad.

AICA organizará su seguridad comprometiendo a todos los miembros del organismo mediante la designación de diferentes roles de seguridad con responsabilidades claramente diferenciadas, tal y como se recoge en el apartado quinto de la presente resolución

8. Autorización y control de los accesos.

AICA implementará mecanismos de control de acceso al sistema de información, limitándolo a los usuarios, procesos, dispositivos y otros sistemas de información, debidamente autorizados, y exclusivamente a las funciones permitidas.

9. Protección de las instalaciones.

C/ INFANTA MERCEDES, 31.
4ª planta
28020 MADRID
Teléfono: 91 347 8369

AICA implementará mecanismos de control de acceso físico, previniendo los accesos físicos no autorizados, así como los daños a la información y a los recursos, mediante perímetros de seguridad, controles físicos y protecciones generales en áreas.

10. Adquisición de productos de seguridad y contratación de servicios de seguridad.

Para la adquisición de productos o contratación de servicios de seguridad, AICA tendrá en cuenta la utilización de forma proporcionada a la categoría del sistema y el nivel de seguridad determinado, aquellos que tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición.

Para la contratación de servicios de seguridad se atenderá a lo señalado en cuanto a la profesionalidad.

11. Protección de la información almacenada y en tránsito y continuidad de la actividad.

AICA prestará especial atención a la información almacenada o en tránsito a través de los equipos o dispositivos portátiles o móviles, los dispositivos periféricos, los soportes de información y las comunicaciones sobre redes abiertas, que deberán analizarse especialmente para lograr una adecuada protección.

Se aplicarán procedimientos que garanticen la recuperación y conservación a largo plazo de los documentos electrónicos producidos por los sistemas de información comprendidos en el ámbito de aplicación del Real Decreto 311/2022, de 3 de mayo, cuando ello sea exigible.

Toda información en soporte no electrónico que haya sido causa o consecuencia directa de la información electrónica a la que se refiere el Real Decreto 311/2022, de 3 de mayo, deberá estar protegida con el mismo grado de seguridad que ésta. Para ello, se aplicarán las medidas que correspondan a la naturaleza del soporte, de conformidad con las normas que resulten de aplicación.

Los sistemas dispondrán de copias de seguridad y se establecerán los mecanismos necesarios para garantizar la continuidad de las operaciones en caso de pérdida de los medios habituales.

12. Registro de actividad y detección de código dañino.

AICA, con el propósito de satisfacer el objeto del Real Decreto 311/2022, de 3 de mayo, con plenas garantías del derecho al honor, a la intimidad personal y familiar y a la propia imagen de los afectados, y de acuerdo con la normativa sobre protección de datos personales, de función pública o laboral, y demás disposiciones que resulten de aplicación, registrará las actividades de los usuarios, reteniendo la información estrictamente necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa.

Al objeto de preservar la seguridad de los sistemas de información, garantizando la rigurosa observancia de los principios de actuación de las Administraciones Públicas, y de conformidad con lo dispuesto en el Reglamento General de Protección de Datos y el respeto a los principios de limitación de la finalidad, minimización de los datos y limitación del plazo de conservación allí enunciados, AICA podrá, en la medida estrictamente necesaria y proporcionada, analizar las comunicaciones entrantes o salientes, y únicamente para los fines de seguridad de la información, de forma que sea posible impedir el acceso no autorizado a las redes y sistemas de información,

C/ INFANTA MERCEDES, 31.
4ª planta
28020 MADRID
Teléfono: 91 347 8369

detener los ataques de denegación de servicio, evitar la distribución malintencionada de código dañino así como otros daños a las antedichas redes y sistemas de información.

Para corregir o, en su caso, exigir responsabilidades, cada usuario que acceda al sistema de información deberá estar identificado de forma única, de modo que se sepa, en todo momento, quién recibe derechos de acceso, de qué tipo son éstos, y quién ha realizado una determinada actividad.

13. Infraestructuras y servicios comunes.

AICA tendrá en cuenta que la utilización de infraestructuras y servicios comunes de las Administraciones Públicas, incluidos los compartidos o transversales.

DECIMOTERCERO. Clasificación de la información.

AICA clasificará e inventariará los activos de la información en virtud de su naturaleza. El nivel de protección y las medidas a aplicar se basarán en el resultado de dicha clasificación. El Responsable de la Información tendrá la potestad de definir esta clasificación.

DECIMOCUARTO. Obligaciones del personal.

Todo el personal de AICA tendrá la obligación de conocer y cumplir esta Política de Seguridad de la Información y la normativa de seguridad, siendo responsabilidad del Responsable de Seguridad disponer los medios necesarios para que la información llegue a los afectados.

Todo el personal de AICA atenderá a una sesión de concienciación en materia de seguridad TIC al menos una vez al año. Se establecerá un programa de concienciación continua, en particular al personal de nueva incorporación.

Las personas con responsabilidad en el uso, operación o administración de sistemas TIC recibirán formación para el manejo seguro de los sistemas en la medida en que la necesiten para realizar su trabajo. La formación será obligatoria antes de asumir una responsabilidad, tanto si es su primera asignación o si se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo.

DECIMOQUINTO. Terceras partes.

Cuando AICA preste servicios a otros organismos o maneje información de otros organismos, se les hará partícipes de esta Política de Seguridad de la Información, se establecerán canales para reporte y coordinación de los respectivos Responsables de Seguridad y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando AICA utilice servicios de terceros o ceda información a terceros, se les hará partícipes de esta Política de Seguridad de la Información y de la normativa de seguridad que ataña a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de reporte y resolución de incidencias. Se garantizará que el personal de terceros está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política.

Cuando algún aspecto de la Política no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se requerirá un informe del Responsable de Seguridad que

C/ INFANTA MERCEDES, 31.
4ª planta
28020 MADRID
Teléfono: 91 347 8369

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 seguir adelante.

DECIMOQUINTO. Efectos y revisión.

La presente "Política de Seguridad de la Información" será aplicable desde la fecha de firma de la presente resolución y será revisada cada año siempre que existan modificaciones estructurales y funcionales de calado que lo aconsejen.

La presente Política no entra en contradicción con ninguna de las disposiciones de la "Política de Seguridad de la Información del Ministerio de Agricultura, Pesca y Alimentación", a la que se encuentra adscrita AICA, prevaleciendo esta última en su caso.

LA DIRECTORA

María Fernández Sanz

C/ INFANTA MERCEDES, 31.
4ª planta
28020 MADRID
Teléfono: 91 347 8369