agroseguro

Política de Seguridad y privacidad de la Información

DGE-N-0010 l Versión 2.1

Fecha entrada en vigor: 29 de noviembre de 2024

Control de versiones

Versión	Fecha aprobación	Cambios
1.0	08/07/2022	Versión inicial
2.0	29/11/2024	Se incluye, en el apartado 9 “Marco normativo”, la referencia al Real Decreto 311/2022 del ENS, sustituyendo al anterior.
		Se sustituye la referencia a la norma ISO 27001:2013 e ISO 27002:2013 por ISO 27001:2022 e ISO 27002:2022 respectivamente.
		Se incluye en todo el documento la aplicación de la norma ISO27701 Gestión de privacidad de la información, esto implica que el término “seguridad de la información” se convierte en “seguridad y privacidad de la información”.
		Se incluye un apartado para incluir el tratamiento de los datos de carácter personal, en cumplimiento de los requisitos del ENS.
2.1	17/03/2026	Actualizado con la plantilla de la nueva imagen corporativa

Ficha de distribución de documento

Nombre/área/compañía	Soporte distribución
Agroseguro	Portal del empleado
Asegurados, entidades, organismos, proveedores y resto de partes	Web corporativa

Índice

1. Ámbito de aplicación

La presente política afecta a todos aquellos sistemas de información que estén dentro del alcance del Sistema de Gestión de Seguridad de la Información de Agroseguro (en adelante SGSI), diseñado en base a los requisitos establecidos en la norma UNE-ISO/IEC 27001 y el Esquema Nacional de Seguridad.

Entendemos por seguridad de la información el conjunto de medidas, principios y controles destinados a proteger los activos de información de la organización frente a amenazas internas o externas, intencionales o accidentales, garantizando su confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad, sea cual sea su formato, ubicación o medio de tratamiento.

2. Misión

La misión de Agroseguro es el diseño y gestión de los seguros agrarios por cuenta de las entidades de seguro integradas en el cuadro de coaseguro de un modo eficiente, sostenible y transparente, contribuyendo al desarrollo económico y social del sector agropecuario, generando valor a sus accionistas y proporcionando a sus trabajadores la posibilidad de desarrollar su creatividad y capacidades profesionales buscando la excelencia en la calidad y el servicio, siendo, además, referente de los seguros agrarios en el contexto internacional.

3. Objetivos

El objetivo de la presente política es impulsar la adopción de una serie de medidas organizativas y técnicas con la finalidad de proteger los recursos de información de Agroseguro, así como los sistemas utilizados para su captura, almacenamiento, procesamiento, transmisión y difusión, frente a amenazas, internas o externas, deliberadas o accidentales, que pudieran comprometer una o varias de las dimensiones de la seguridad de la información establecidas en el SGSI:

- *Confidencialidad:* la información perteneciente a Agroseguro debe ser conocida exclusivamente por las personas autorizadas, previa identificación en el momento y por los medios habilitados.
- *Integridad:* la información de Agroseguro debe ser completa, exacta y válida, siendo su contenido el facilitado por los afectados sin ningún tipo de manipulación.
- *Disponibilidad:* la información de Agroseguro debe estar accesible y utilizable por los usuarios autorizados e identificados en todo momento, quedando garantizada su propia persistencia ante cualquier eventualidad prevista.
- *Autenticidad:* Agroseguro debe poder identificar o garantizar que el origen y destinatario de la información son quien dicen ser.
- *Trazabilidad:* Agroseguro debe poder registrar e identificar las acciones realizadas sobre la información.

4. Principios de la seguridad y la privacidad de la información

Las directrices fundamentales de seguridad se concretan en los siguientes principios:

a) **Alcance estratégico**: la seguridad y la privacidad de la información debe contar con el compromiso y apoyo de todos los niveles directivos, de forma que pueda estar coordinada e integrada con el resto de iniciativas estratégicas.

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

c) **Seguridad integral**: la seguridad se entenderá como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con el sistema, evitando, salvo casos de urgencia o necesidad, cualquier actuación puntual o tratamiento coyuntural. La seguridad y la privacidad de la información debe considerarse como parte de la operativa habitual, estando presente y aplicándose desde el diseño inicial de los sistemas de información.

d) **Seguridad por defecto**: los sistemas deben diseñarse y configurarse de forma que garanticen un grado suficiente de seguridad por defecto.

e) **Seguridad física**: los activos de información serán emplazados en áreas seguras, protegidas por controles de acceso físicos adecuados a su nivel de criticidad. Los sistemas y los activos de información que contienen dichas áreas estarán suficientemente protegidos frente a amenazas físicas o ambientales.

f) **Seguridad en la gestión de comunicaciones y operaciones**: se establecerán los procedimientos necesarios para lograr una adecuada gestión de la seguridad, operación y actualización de las Tecnologías de la Información y Comunicaciones. La información que se transmita a través de redes de comunicaciones deberá ser adecuadamente protegida, teniendo en cuenta su nivel de sensibilidad y de criticidad, mediante mecanismos que garanticen su seguridad.

g) **Control de acceso**: se limitará el acceso a los activos de información por parte de usuarios, procesos y otros sistemas de información mediante la implantación de los mecanismos de identificación, autenticación y autorización acordes a la criticidad de cada activo. Además, quedará registrada la utilización del sistema con objeto de asegurar la trazabilidad del acceso y auditar su uso adecuado, conforme a la actividad de la organización.

h) **Adquisición de productos y servicios de seguridad**: en la adquisición de productos que vayan a ser utilizados por el organismo, se utilizarán aquellos que tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición, salvo en aquellos casos en que las exigencias de proporcionalidad en cuanto a los riesgos asumidos no lo justifiquen. Para la contratación de servicios de seguridad el organismo exigirá de manera objetiva y no discriminatoria que las organizaciones que les presten servicios de seguridad

cuenten con profesionales cualificados y con unos niveles idóneos de gestión y madurez en los servicios prestados.

i) **Incidentes de seguridad**: se dispondrá de procedimientos dirigidos a la correcta identificación, registro y resolución de los incidentes de seguridad.

j) **Continuidad de la actividad**: se implantarán los mecanismos apropiados para asegurar la disponibilidad de los sistemas de información y mantener la continuidad de sus procesos de negocio, de acuerdo con las necesidades de nivel de servicio de sus usuarios.

k) **Cumplimiento**: la Dirección se compromete a cumplir con los requisitos y objetivos de seguridad establecidos, así como a cumplir con los requisitos legales o reglamentarios que le sean de aplicación.

l) **Mejora continua:** Agroseguro evaluará, de forma periódica, la información y la eficacia del SGSI, adecuando la misma a la constante evolución de los riesgos y sistemas de protección.

5. Estructura Organizativa

La estructura organizativa para la gestión de la seguridad y la privacidad de la información está compuesta por los siguientes actores:

- Responsable de Seguridad
- Responsable del Sistema de Información
- Responsables de la Información
- Responsable del Servicio
- Responsable de Tratamiento de datos personales
- Delegado de la Protección de Datos
- Comité de Seguridad de la Información

A continuación, se describen las responsabilidades de cada uno de ellos.

5.1 Responsable de Seguridad

El Responsable de Seguridad es la persona que toma las decisiones para satisfacer los requisitos de seguridad y privacidad de la información y de los servicios, siendo el de mayor responsabilidad dentro del sistema.

Serán funciones del Responsable de Seguridad:

- Elaborar la estrategia de evolución de la organización, en lo que respecta a seguridad y privacidad de la información;
- Supervisar el cumplimiento de la Política de Seguridad, así como de sus normas y procedimientos derivados;
- Conocer y supervisar la investigación y monitorización de los incidentes de seguridad;
- Aprobar las medidas que permitan cumplir los requisitos de seguridad establecidos por el Responsable del Servicio y los de la Información;

- Promover la gestión de riesgos y su análisis;
- Monitorizar el estado de seguridad del sistema proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría implementados;
- Promover las actividades de concienciación y formación en materia de seguridad;
- Promover la realización de las auditorias periódicas que permitan verificar el cumplimiento de las obligaciones del organismo en materia de seguridad;
- Informar regularmente del estado de la seguridad y la privacidad de la información a la Dirección;
- Preparar los temas a tratar en las reuniones del Comité de Seguridad de la Información, aportando información puntual para la toma de decisiones;
- Aprobar los procedimientos de seguridad elaborados por el responsable del Sistema de Información.
- Presidir el Comité de Seguridad.

5.2 Responsable de la Información

Los Responsables de la Información tienen la potestad de establecer los requisitos, en materia de seguridad, de la información que manejan. Si esta información incluye datos de carácter personal, deberán tener en cuenta las medidas de seguridad que corresponda implantar atendiendo a los riesgos generados por el tratamiento de acuerdo con lo exigido en el Reglamento (UE) 2016/679 DEL Parlamento Europeo y del Consejo del 27 de abril de 2016 y demás legislación aplicable en materia de protección de datos de carácter personal.

5.3 Responsable del Servicio

El Responsable del Servicio tiene la potestad de establecer los requisitos, en materia de seguridad, de los servicios que se prestan desde el área de Tecnología y Procesos, de forma que queden cubiertas las necesidades del cliente y de los usuarios del servicio, Si esta información incluye datos de carácter personal, deberán tener en cuenta las medidas de seguridad que corresponda implantar atendiendo a los riesgos generados por el tratamiento de acuerdo a lo exigido en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo del 27 de abril de 2016 y demás legislación aplicable en materia de protección de datos de carácter personal.

5.4 Responsable del Sistema de Información

El Responsable del Sistema de Información se encarga de desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida.

Serán funciones del Responsable del Sistema de Información:

- Garantizar que las medidas de seguridad se integran adecuadamente dentro del marco general de la seguridad y la privacidad de la información;
- Aprobar toda modificación sustancial de la configuración de cualquier elemento del sistema;
- Elaborar procedimientos técnicos de seguridad de los sistemas de información;
- Elaborar planes de continuidad de los sistemas de información;
- Colaborar para la realización del análisis de riesgos de los sistemas de información de los que es responsable;

- Implementar, gestionar y mantener las medidas de seguridad aplicables al sistema de información;
- Gestionar, configurar y actualizar, en su caso, el hardware y software en los que se basan los mecanismos y servicios de seguridad del sistema de información;
- Proponer la suspensión del tratamiento de una cierta información o la prestación de un determinado servicio si aprecia deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos.

5.5 Responsable del Tratamiento de Datos Personales

Las funciones del Responsable del Tratamiento de Datos Personales serán las indicadas en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 y demás disposiciones reguladoras de la materia, entre las que cabe destacar:

- Aplicar las medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que los tratamientos que lleva a cabo son conformes con la normativa legal vigente en materia de protección de datos de carácter personal.
- Designar al Delegado de Protección de Datos e informar de su nombramiento y cese a la Agencia Española de Protección de Datos.

5.6 Delegado de Protección de Datos

Las funciones del Delgado de Protección de Datos serán las indicadas en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 y demás disposiciones reguladoras de la materia.

5.7 Comité de Seguridad de la Información

El Comité de Seguridad de la Información está formado por el Responsable de Seguridad, el Responsable del Sistema de Información y el Delegado de la Protección de Datos.

El Comité es un órgano establecido para la coordinación y la supervisión del sistema de gestión de la seguridad y la privacidad de la información.

Dentro de las funciones del Comité de Seguridad de la Información se contemplan:

- Elaborar y revisar, a intervalos planificados, la Política de Seguridad y el Manual de Seguridad;
- Establecer y revisar anualmente los objetivos de seguridad, en consonancia con la Política de Seguridad;
- Supervisar la información documentada que se elabore para regular el funcionamiento del SGSI;
- Aprobar y hacer seguimiento de los planes de mejora de la seguridad y la privacidad de la información de la organización, así como de los planes de acción derivados de las auditorias.
- Priorizar las actuaciones en materia de seguridad, cuando los recursos sean limitados.
- Velar porque la seguridad y la privacidad de la información se tenga en cuenta en todos los proyectos TIC desde su especificación inicial hasta su puesta en producción.

- Supervisar la metodología de Gestión de Riesgos, los resultados de la Evaluación del Riesgo y los Planes de Tratamiento de Riesgos que se deriven de sucesivas revisiones del SGSI;
- Revisar y monitorizar los incidentes de seguridad y privacidad de la información, y recomendar posibles actuaciones respecto de ellos.
- Revisar las métricas e indicadores de seguridad.
- Definir las necesidades de asesoramiento por parte de especialistas externos en materia de seguridad y privacidad de la información;
- Promover la mejora continua del sistema de gestión de la seguridad de la información.

El Comité de Seguridad se reunirá con carácter ordinario al menos una vez al año, y con carácter extraordinario cuando lo decida su Presidente.

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

5.8 Procedimiento de designación

El Responsable de Información, el Responsable de Servicio, el Responsable de Seguridad y el Delegado de Protección de Datos son designados por la Dirección General de Agroseguro, teniendo igualmente la potestad de renovarlos o cesarlos.

El Responsable de Sistemas de Información es designado por el Responsable de Seguridad, quien tiene potestad de renovarlos o cesarlos.

6. Tratamiento de datos de carácter personal

Agroseguro solo recogerá y tratará datos de carácter personal cuando sean adecuados, pertinentes y no excesivos y estos se encuentren en relación con el ámbito y las finalidades para los que se hayan obtenido.

De igual modo, adoptará las medidas de índole técnicas y organizativas necesarias para el cumplimiento de la normativa de Protección de Datos vigente en cada caso, adoptando medidas tales como: el análisis de legitimidad jurídica de cada uno de los datos tratamientos de datos que se lleven a cabo, el análisis de riesgos, la evaluación de impacto cuando el riesgo ha sido alto, el registro de actividades de tratamiento y el nombramiento del Delegado de Protección de Datos.

7. Obligaciones del personal

El personal de Agroseguro tendrá la obligación de conocer y cumplir, además de la presente política, todas las directrices generales, normas y procedimientos de seguridad y privacidad de la información que puedan afectar a sus funciones.

Todos los miembros de Agroseguro recibirán formación en seguridad y privacidad de la información. Se establecerá un programa de concienciación continua para atender a todos los miembros de Agroseguro, en particular a los 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.

8. Estructura de la Documentación

El cuerpo normativo sobre la seguridad y la privacidad de la información se desarrollará en tres niveles:

a) **Primer nivel normativo**: constituido por la Política de Seguridad de la Información, la cual debe ser adecuada a los fines de Agroseguro, y estará alineada con el contexto de la estrategia de gestión del riesgo de la Organización dentro del cual se establecerá y mantendrá el Sistema de Gestión de Seguridad de la Información.

La aprobación de la Política de Seguridad de la Información recae en la Dirección General de Agroseguro y tendrá carácter imperativo sobre toda la organización.

b) **Segundo nivel normativo:** constituido por las normas, políticas particulares y procedimientos de seguridad desarrollados por Agroseguro, que tendrán que cumplir con lo indicado en el primer nivel normativo. Dentro de este nivel tiene especial relevancia el Manual de Seguridad de la Información, donde se describe el Sistema de Gestión de Seguridad de la Información (SGSI) establecido en Agroseguro, incluyendo su alcance, de acuerdo con la Norma internacional ISO/IEC 27001:2022 y la Norma de Seguridad de la Información basada en la Norma internacional ISO/IEC 27002:2022**.**

c) **Tercer nivel normativo:** instrucciones técnicas y documentos auxiliares Son documentos que, cumpliendo con lo expuesto en la Política del Sistema de Información, determinan las acciones o tareas a realizar en el desempeño de un proceso. Tendrán que cumplir estrictamente con lo indicado con el primer y segundo nivel normativo.

9. Marco Normativo

El marco legal y regulatorio en el que desarrollamos nuestras actividades es el siguiente:

- ✓ Ley 50/1980, de 8 de octubre, de Contrato de Seguro.
- ✓ Ley 87/1978, de 28 de diciembre, de Seguros Agrarios Combinados.
- ✓ Real Decreto 2329/1979, de 14 de septiembre, por el que se aprueba el Reglamento para aplicación de la Ley 87/1978, de 28 de diciembre, sobre Seguros Agrarios Combinados
- ✓ Real Decreto 1468/2001 de 27 de diciembre, por el que se modifica el reglamento para aplicación de la Ley 87/1978
- ✓ Real Decreto 288/2021, de 20 de abril, por el que se modifica el Real Decreto 1060/2015, de 20 de noviembre, de ordenación, supervisión y solvencia de las entidades aseguradoras y reaseguradoras.

- ✓ Real Decreto 425/2016, de 11 de noviembre, por el que se establecen las bases reguladoras para la concesión de subvenciones de la Administración General del Estado al Seguro Agrario.
- ✓ 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.
- ✓ Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- ✓ Real Decreto 311/2022, de 3 de mayo, de desarrollo del Esquema Nacional de Seguridad que sustituye, a su vez, al Real Decreto 3/2010, de 8 de enero.
- ✓ Órdenes por las que se establece el sistema de reaseguro a cargo del Consorcio de Compensación de Seguros para el correspondiente Plan de Seguros Agrarios Combinados.
- ✓ Resoluciones de la Subsecretaría del Ministerio de Agricultura, Pesca y Alimentación, por la que se aprueba los correspondientes Planes de Seguros Agrarios Combinados.

Además de la normativa indicada, en el Manual de Seguridad de la información, documento de uso interno, se especifican el resto de las normativas a las que Agroseguro está sujeto.

10. Aprobación y entrada en vigor

Esta Política de Seguridad ha sido aprobada por la Dirección General de Agroseguro, siendo efectiva desde dicha fecha y hasta que sea reemplazada por una nueva versión.