Política de Seguridad

Versión 0.1

Fecha aprobación: 01/06/2026

Estado: Aprobado

open sistemas

Control de Versiones

Versión	Autor	Descripcón	Fecha de Entrega
1.0	Seven Weeks	Versión Inicial	Enero 2026

Responsabilidades

Acción	Nombre	Compñía	Fecha
Realizada por	Equipo Consultor	Seven Weeks	Enero 2026
Revisado por	Equipo Interno	OpenSistemas	Mayo 2026
Aprobado por	Dirección	OpenSistemas	Junio 2026

Documentos de referencia

Documento	Comentarios
Artículo 12 Política de Seguridad	BOE
5.1 Políticas para la Seguridad de la Información	ISO 27002:2022 (Bloque 5. Organización)
5.2 Roles y Responsabilidades en Seguridad de la Información	ISO 27002:2022 (Bloque 5. Organización)
5.5 Responsabilidades de la Dirección	ISO 27002:2022 (Bloque 5. Organización
5.6 Contacto con Grupos de Interés Especial	ISO 27002:2022 (Bloque 5. Organización)

Calificación del documento

<table>
<tr><th colspan="2">Difusión</th><th colspan="2">Seguridad</th></tr>
<tr><td>IN1 Interna</td><td rowspan="3">IN3</td><td>NL1: General</td><td rowspan="3">NL1</td></tr>
<tr><td>IN2 Clientes</td><td>NL2: Restringido</td></tr>
<tr><td>IN3 Exterior</td><td>NL3: Confidencial</td></tr>
</table>

Contenido

1.- Principios básicos y seguridad

- Artículo 5: La seguridad debe considerarse de forma global, abarcando todos los aspectos de la organización, sus sistemas, servicios, personas, instalaciones y recursos.
- Artículo 6: Todas las medidas de seguridad deben fundamentarse en el análisis y la gestión de riesgos, priorizando aquellos que puedan impactar más gravemente.
- Artículo 7: Las políticas de seguridad deben contemplar mecanismos para prevenir incidentes, detectarlos de manera temprana, responder eficazmente y garantizar la recuperación.
- Artículo 8: Implementar líneas de defensa que aseguren redundancia y refuercen la seguridad en distintos niveles y capas.
- Artículo 9: Las políticas y medidas de seguridad deben revisarse de manera periódica para adaptarse a los cambios en el entorno, los riesgos y las amenazas.
- Artículo 10: Las responsabilidades en materia de seguridad deben estar claramente asignadas, evitando conflictos de interés y asegurando la independencia en las funciones de supervisión y ejecución.
- Artículo 11: La política de seguridad y las medidas implementadas deben estar debidamente documentadas, actualizadas y ser objeto de mejora continua.

Además, el tratamiento de los datos personales se realizará conforme a los principios de:

- Licitud, lealtad y transparencia.
- Limitación de la finalidad y minimización de datos.
- Exactitud y actualización de la información personal.
- Integridad, confidencialidad y disponibilidad de los datos personales.
- Limitación del plazo de conservación y supresión o bloqueo cuando proceda.
- Privacidad desde el diseño y por defecto en procesos, servicios, sistemas y desarrollos.

La presente Política Integrada establece el marco general para la protección de la información y de los datos personales tratados por OPENSISTEMAS, garantizando el cumplimiento de la normativa aplicable en materia de seguridad de la información, privacidad y protección de datos personales.

2.- Organización e implementación del proceso de seguridad (art.13)

Esta “Política de Seguridad de la Información” es efectiva desde su entrada en vigor el día 1 de junio de 2026 por OPEN SISTEMAS.

La Política es revisada por el responsable de Seguridad de la Información a intervalos planificados, sin exceder el año de duración, o siempre que se produzcan cambios significativos, a fin de asegurar que se mantenga su idoneidad, adecuación y eficacia.

La seguridad de los sistemas de información deberá comprometer a todos los miembros de la organización, comunicándose de forma efectiva.

Los cambios sobre la Política de Seguridad de la Información serán aprobados por la Dirección de OPEN SISTEMAS. Cualquier cambio sobre la misma deberá ser difundido para conocimiento de toda la Organización.

La dirección de la empresa es consciente del valor de la información y está profundamente comprometida con la política descrita en este documento.

Esta Política es de aplicación a todas las sociedades filiales o participadas mayoritariamente sobre las que OPEN SISTEMAS ejerza, directa o indirectamente, un control efectivo, a los miembros de los órganos de administración, directivos y empleados del Grupo, con independencia de su ubicación geográfica, y a terceros que mantengan relaciones con el Grupo en aquellos aspectos que les resulten de aplicación.

En el desarrollo de actividades fuera de España, esta Política se adaptará a la legislación local que resulte aplicable, atendiendo siempre al criterio más restrictivo en materia de seguridad y protección de datos.

3.- Misión

El propósito de esta Política de Seguridad de la Información es proteger la información de los servicios de OPEN SISTEMAS.

La política de Seguridad, junto con la Normativa de Seguridad se realizará mediante una comunicación a todos los trabajadores, para que se efectúe el análisis, comprensión y lectura del documento.

Esta política aplica al sistema de información propiedad de OPEN SISTEMAS, para la adecuada prestación de los servicios y soluciones basadas en tecnologías de código abierto, a través de sus líneas de negocio de Soluciones, Servicios Gestionados y Soporte.

Asimismo, la presente Política tiene como finalidad establecer los principios, compromisos y directrices en materia de Seguridad de la Información y Protección de Datos Personales aplicables en OpenSistemas (y, en su caso, las entidades sobre las que ejerza control operativo o societario cuando resulte aplicable), garantizar la confidencialidad, integridad, disponibilidad, trazabilidad y autenticidad de la información tratada por la organización, asegurar el tratamiento lícito, leal y transparente de los datos personales de clientes, proveedores, empleados y demás partes interesadas, dar cumplimiento a los requisitos legales, normativos, contractuales y regulatorios aplicables y promover una cultura de seguridad, privacidad y mejora continua en todos los niveles de la organización.

4.- Funciones de seguridad

OPEN SISTEMAS ha nombrado un COMITÉ de Seguridad con sus Funciones y Responsabilidades.

El establecimiento de este comité, así como la designación de los diferentes roles se hallan registrados en el Acta de Constitución del comité: **OS_Acta de Constitución_ENS_v1** y en **Acta de Nombramientos: OS_Aceptación de Roles y Funciones_v1.**

Se añade, por el alcance integrado de esta política, la figura del Responsable de Seguridad del Tratamiento para las funciones específicas de control del tratamiento de datos personales.

El Comité de Seguridad de la Información del ENS está formado por:

- Responsable de Seguridad
- Responsable de Sistemas
- Responsable de la Información
- Responsable del Servicio
- Responsable de Seguridad del Tratamiento
- Delegado de Protección de Datos (DPD)

Se deben identificar unos claros responsables para velar por su cumplimiento y ser conocida por todos los miembros de la organización. Se detallarán en la política de seguridad de la organización las atribuciones de cada responsable.

Los nombramientos los establece la Dirección de la organización y se revisan cada 2 años o cuando un puesto queda vacante. Las diferencias de criterios que pudiesen derivar en un conflicto se tratarán en el seno del Comité de Seguridad y prevalecerá en todo caso el criterio de la Dirección.

Los diferentes roles junto con sus respectivas funciones y responsabilidades:

El **Responsable de la Información** tendrá como funciones:

- Aceptar los riesgos residuales respecto de la información, calculados en el análisis de riesgos.
- Aunque la aprobación formal de los niveles corresponda al responsable de la Información, se puede recabar una propuesta al responsable de la Seguridad y conviene que se escuche la opinión del Responsable del Sistema.
- Determinar los requisitos de la información tratada.
- Velar por la seguridad de la información en sus diferentes vertientes: protección física, protección de los servicios y respeto de la privacidad.
- Estar al tanto de cambios normativos (leyes, reglamentos o prácticas sectoriales) que afecten a la Organización
- Adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.

El **Responsable del servicio** tendrá las funciones:

- Determinar los requisitos de Seguridad de los servicios prestados en los Clientes.
- Revisar y aprobar los niveles de seguridad de los servicios.
- Incluir las especificaciones de seguridad en el ciclo de vida de los servicios y sistemas, acompañadas de los correspondientes procedimientos de control.
- Valorará las consecuencias de un impacto negativo sobre la seguridad de los servicios, se efectuará atendiendo a su repercusión en la capacidad de la organización para el logro de sus objetivos, la protección de sus activos, el cumplimiento de sus obligaciones de servicio, el respeto de la legalidad y los derechos de los Clientes.
- Asumir la propiedad de los riesgos sobre los servicios.

El **Responsable de sistemas** tendrá las funciones:

- Desarrollar, operar y mantener el Sistema durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.
- Definir la topología y política de gestión del Sistema estableciendo los criterios de uso y los servicios disponibles en el mismo.
- Definir la política de conexión o desconexión de equipos y usuarios nuevos en el Sistema.
- Implantar y controlar las medidas específicas de seguridad del Sistema y cerciorarse de que éstas se integren adecuadamente dentro del marco general de seguridad.
- Determinar la configuración autorizada de hardware y software a utilizar en el Sistema.
- Aprobar toda modificación sustancial de la configuración de cualquier elemento del Sistema.
- Llevar a cabo el proceso de análisis y gestión de riesgos en el Sistema.
- Determinar la categoría del sistema y determinar las medidas de seguridad que deben aplicarse Elaborar y aprobar la documentación de seguridad del Sistema.
- Investigar los incidentes de seguridad que afecten al Sistema, y en su caso, comunicación al responsable de Seguridad.
- Establecer planes de contingencia y emergencia, llevando a cabo frecuentes ejercicios para que el personal se familiarice con ellos.

El **Responsable de seguridad** tendrá las funciones:

- Responsable de la Seguridad es la persona designada por la Dirección de la Organización.
- Determinar las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios.
- Trabajar para conseguir una total seguridad de los datos de la empresa, así como la privacidad de los mismos.
- Supervisar, controlar y administrar el acceso a la información de la empresa, y de sus trabajadores.
- Elaborar un conjunto de medidas de respuesta ante incidentes de seguridad relacionados con la información, incluyendo la recuperación ante desastres.
- Garantizar el cumplimiento de la normativa relacionada con la seguridad de la información.
- En caso de servicios externalizados, la responsabilidad última la tiene siempre la Organización destinataria de los servicios, aun cuando la responsabilidad inmediata pueda corresponder (vía contrato) a la organización prestataria del servicio.

- Mantener la seguridad de la información manejada y de los servicios prestados por los Sistemas de información en su ámbito de responsabilidad, de acuerdo con lo establecido en la Política de Seguridad de la organización.
- Sistemas de información en su ámbito de responsabilidad, de acuerdo con lo establecido en la Política de Seguridad de la Información de la organización.
- Promover la formación y concienciación en materia de seguridad de la información.
- Garantizar el buen uso del equipamiento informático dentro de su ámbito de responsabilidad.
- Supervisar y coordinar al equipo encargado de llevar a cabo las medidas de respuesta en caso de brechas de seguridad.
- POC (Persona de contacto de seguridad de la información) Se responsabilizará de la seguridad con los Clientes, en los que presta servicio OPEN SISTEMAS.
- Realizar operaciones de seguridad para luchar contra el fraude y el robo de información.
- Diseñar del Plan de formación, en el ámbito del ENS, para las personas de OPEN SISTEMAS que prestan servicios en proyectos de AA.PP.

Responsable de Seguridad del Tratamiento

- Supervisar que los datos personales se tratan de forma lícita y con una finalidad determinada.
- Verificar la adecuación y actualización de los datos personales.
- Controlar la supresión o bloqueo de los datos que hayan dejado de ser necesarios.
- Comprobar la existencia del consentimiento u otra base legal válida para el tratamiento.
- Garantizar el cumplimiento del deber de información.
- Atender las solicitudes de ejercicio de derechos de los interesados a través del canal habilitado por la organización.
- Verificar la legalidad y seguridad de las transferencias internacionales de datos.

El **DPD** tendrá las funciones

- Informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben en virtud del presente Reglamento y de otras disposiciones de protección de datos de la Unión o de los Estados miembros.
- Supervisar el cumplimiento de lo dispuesto en el presente Reglamento, de otras disposiciones de protección de datos de la Unión o de los Estados miembros y de las

políticas del responsable o del encargado del tratamiento en materia de protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes.

- Ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación de conformidad con el artículo 35.
- Cooperar con la autoridad de control.
- Actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa a que se refiere el artículo 36, y realizar consultas, en su caso, sobre cualquier otro asunto.
- Desempeñará sus funciones prestando la debida atención a los riesgos asociados a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y fines del tratamiento.

5.- Reportes

El administrador de seguridad reporta al Responsable del Sistema o al Responsable de la Seguridad, según sea su dependencia funcional:

- Incidentes relativos a la seguridad del sistema o acciones de configuración, actualización o corrección.
- El Responsable del Sistema informa al Responsable de la Información de las incidencias funcionales relativas a la información que le compete.
- El Responsable del Sistema informa al Responsable del Servicio de las incidencias funcionales relativas al servicio que le compete.
- El Responsable del Sistema reporta al Responsable de la Seguridad: actuaciones en materia de seguridad, en particular en lo relativo a decisiones de arquitectura del sistema
- Resumen consolidado de los incidentes de seguridad.
- Las brechas de seguridad que afecten a datos personales deberán escalarse además de acuerdo con el procedimiento de gestión de violaciones de seguridad de los datos personales.

6.- Análisis y gestión de los riesgos (art. 14)

Se realizará un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos. Este análisis será la base para determinar las medidas de seguridad que se deben adoptar, además de los mínimos establecidos según lo previsto en el artículo 7 y 14 del BOE, se repetirá:

- Regularmente, al menos una vez al año.
- Cuando cambie la información manejada.
- Cuando cambien los servicios prestados.
- Cuando ocurra un incidente grave de seguridad.
- Cuando se reporten vulnerabilidades graves.
- Cuando haya un incidente de seguridad relacionado con la normativa LOPDGDD
- Cuando haya una brecha de seguridad relacionada con la información tratada de un usuario según la normativa LOPDGDD.

Los criterios de evaluación de riesgos se especificarán en la metodología de evaluación de riesgos y de incidentes de seguridad que elaborará la organización, basándose en estándares, buenas prácticas reconocidas y normas jurídicas.

Deberán tratarse, como mínimo, todos los riesgos que puedan impedir la prestación de los servicios o el cumplimiento de la misión de la organización de forma grave. Se priorizarán especialmente los riesgos que impliquen un cese en la prestación de servicios, o repercuta a dicha información tratada durante el servicio.

Los criterios de evaluación de riesgos se especificarán en la metodología de evaluación de riesgos que elaborará la organización, basándose en estándares y buenas prácticas reconocidas. Deberán tratarse, como mínimo, todos los riesgos que puedan impedir la prestación de los servicios o el cumplimiento de la misión de la organización de forma grave. Se priorizarán especialmente los riesgos que impliquen un cese en la prestación de servicios de OPEN SISTEMAS en los Clientes.

El propietario de un riesgo debe ser informado de los riesgos que afectan a su propiedad y del riesgo residual al que está sometida. Cuando un sistema de información entra en operación, los riesgos residuales deben haber sido aceptados formalmente por su correspondiente propietario.

7.- Gestión de personal (art. 15)

El personal, propio o ajeno, relacionado con los sistemas de información sujetos a lo dispuesto en este real decreto 311/2022, deberá ser formado e informado de sus deberes, obligaciones y responsabilidades en materia de seguridad.

Su actuación, deberá ser supervisada para verificar que se siguen los procedimientos establecidos, aplicará las normas y procedimientos operativos de seguridad aprobados en el desempeño de sus cometidos.

Desde su incorporación, el personal recibirá formación específica en seguridad de la información, GDPR/RGPD, protección de datos y privacidad de la información.

8.- Profesionalidad (art. 16)

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, despliegue, explotación, mantenimiento, gestión de incidencias y desmantelamiento.

Las entidades del ámbito de aplicación de este real decreto exigirán, 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.

9.- Autorización y control de los accesos (art. 17)

El acceso controlado a los sistemas de información comprendidos en el ámbito de aplicación de este real decreto deberá estar limitado a los usuarios, procesos, dispositivos u otros sistemas de información, debidamente autorizados, y exclusivamente a las funciones permitidas.

Los privilegios de acceso de un recurso (persona) al sistema de información de OPEN SISTEMAS, quedan restringidos por defecto al mínimo necesario para el desarrollo de sus funciones.

El sistema de información de OPEN SISTEMAS se mantendrá siempre configurado, de tal manera que evite que un recurso (persona) pueda acceder accidentalmente a recursos con derechos distintos de los autorizados.

10.- Protección de las instalaciones (art. 18)

Los sistemas de información y su infraestructura de comunicaciones asociados a OPEN SISTEMAS deberán permanecer en áreas controladas y disponer de los mecanismos de acceso adecuados y proporcionales en función del análisis de riesgos, sin perjuicio de lo establecido en la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas y en el Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas.

11.- Adquisición de productos de seguridad y contratación de servicios de seguridad (art. 19)

En la adquisición de productos de seguridad o contratación de servicios de seguridad de las tecnologías de la información y la comunicación que vayan a ser empleados en los sistemas de información del ámbito de aplicación de este real decreto, se utilizarán, de forma proporcionada a la categoría del sistema y el nivel de seguridad determinados, aquellos que tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición.

El Organismo de Certificación del Esquema Nacional de Evaluación y Certificación de Seguridad de las Tecnologías de la Información del Centro Criptológico Nacional (en adelante, CCN), constituido al amparo de lo dispuesto en el artículo 2.2.c) del Real Decreto 421/2004, de 12 de marzo, por el que se regula el Centro Criptológico Nacional, teniendo en cuenta los criterios y metodologías de evaluación nacionales e internacionales reconocidas por este organismo y en función del uso previsto del producto o servicio concreto dentro de sus competencias, determinará los siguientes aspectos:

a) Los requisitos funcionales de seguridad y de aseguramiento de la certificación.
b) Otras certificaciones de seguridad adicionales que se requieran normativamente.
c) Excepcionalmente, el criterio a seguir en los casos en que no existan productos o servicios certificados.

Para la contratación de servicios de seguridad se estará a lo señalado en los apartados anteriores y a lo dispuesto en el artículo 16.

Los terceros deberán asumir contractualmente las obligaciones de seguridad, confidencialidad, protección de datos y continuidad que les resulten aplicables.

12.- Registro de la actividad y detección de código dañino (art. 24)

Con el propósito de satisfacer el objeto de este real decreto, 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, se registrarán 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 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, los sujetos comprendidos en el artículo 2 podrán, 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, 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.- Incidentes de seguridad (art. 25)

La entidad titular de los sistemas de información del ámbito de este real decreto dispondrá de procedimientos de gestión de incidentes de seguridad de acuerdo con lo previsto en el artículo 33, la Instrucción Técnica de Seguridad correspondiente y, en caso de tratarse de un operador de servicios esenciales o de un proveedor de servicios digitales, de acuerdo con lo previsto en el anexo del Real Decreto 43/2021, de 26 de enero , por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.

Asimismo, se dispondrá de mecanismos de detección, criterios de clasificación, procedimientos de análisis y resolución, así como de los cauces de comunicación a las partes interesadas y el registro de las actuaciones. Este registro se empleará para la mejora continua de la seguridad del sistema.

Los incidentes con impacto en datos personales se gestionarán adicionalmente conforme a la normativa de protección de datos y a los procedimientos de notificación que resulten de aplicación.

14.- Continuidad de la actividad (art. 26)

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.

La organización establecerá planes de contingencia y emergencia, llevando a cabo frecuentes ejercicios para que el personal se familiarice con ellos.

15.- Mejora continua del proceso de seguridad (art. 27)

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.

16.- Referencia documental

- Políticas de Seguridad ISO 27001
- OS_Normativa de Seguridad
- OS_(INV)_Inventario de Procedimientos
- Registros de actividades de tratamiento y documentación de protección de datos.
- Acta de Constitución del Comité de Seguridad y Acta de Aceptación de Roles y Funciones.

17.- Referencia documental

Documento: Política de Seguridad

Estado: Aprobado

Fdo.